TAKSHASHILA INSTITUTION

Starlink and Risks for India

An assessment of the risks posed by Starlink and recommendations for India

Ashwin Prasad Rao, Aditya Ramanathan, Col. Das (Retd.)

Takshashila Discussion Document 2026-12

Version 1.0, April 2026.

Starlink poses significant risks to India: it can deny connectivity when India needs it, or keep services active when India wants them shut down. India's Global Mobile Personal Communication by Satellite regulatory conditions are a serious effort but insufficient, as operational control of the constellation remains with SpaceX. India should bolster Digital Bharat Nidhi to expand broadband access, prioritise satellite vendors that offer India greater leverage, diversify usage to reduce over-exposure, discourage general retail use of Starlink at this time, and proactively develop a regulatory framework for direct-to-device satellite technology.

Recommended Citation: Ashwin Prasad Rao, Aditya Ramanathan, Col. Das (Retd.), ``Starlink and Risks for India'', Takshashila Discussion Document 2026-12, Version 1.0, April 2026. The Takshashila Institution.

Contents

1 Executive Summary

- Starlink represents significant risks to India.
- It can potentially leverage data from its services in ways that are contrary to the interests of Indians.
- The risks from Starlink stem from its technological lead, Elon Musk's influence on the US government, and his erratic conduct.
- India has imposed stringent security conditions on Global Mobile Personal Communication by Satellite (GMPCS) licensees, but these conditions rely heavily on self-certification and are difficult to enforce independently. The core risks persist despite the regulatory framework.
- India should bolster the Digital Bharat Nidhi scheme to expand broadband access in underserved areas and reduce demand for pricier satellite internet services.
- India can continue using satellite internet for functions such as disaster relief while diversifying vendors to reduce over-exposure.

2 Introduction

Starlink is the world's largest satellite constellation, with over 10,000 active satellites in low Earth orbit (LEO).[1] These currently account for nearly two-thirds of all operational satellites in orbit.[2] Starlink ultimately plans to field as many as 42,000 satellites.[3]

While there are multiple satellite internet constellations being assembled in orbit, including two large Chinese projects, Starlink is the most ambitious and the most advanced. Its dense network of LEO satellites enable high-bandwidth, low latency internet access. Unlike many others, its constellation is also fully operational. Starlink has accomplished this through a focus on scale and vertical integration. Its satellites are designed to be compact and are mass-produced at parent company SpaceX's own facilities. SpaceX's reusable Falcon 9 and Falcon Heavy boosters have also helped substantially reduce the cost of placing satellites into orbit. By 2025, Starlink was adding over 3,000 satellites to orbit each year.[4]

Starlink is operated by Starlink Services, LLC, a wholly owned subsidiary of SpaceX, formally known as Space Exploration Technologies Corp.[5] SpaceX was founded by entrepreneur Elon Musk and remains privately held. A February 2026 merger with Elon Musk's artificial intelligence venture xAI then valued the combined entity at approximately $1.25 trillion.[6] Musk holds an estimated 42–43% of SpaceX's equity. Through a dual-class share structure, he controls approximately 79% of the voting rights.[7]

3 Identifying the Risks

The primary risk with Starlink is the limits it places on the Government of India's ability to manage its availability. ***Starlink services may remain illegally active when the Government wants them to be halted in an area. Conversely, Starlink services may be halted when the Government needs them to be operational.*** An additional risk is that Starlink may leverage sensitive data from its users for intelligence purposes or commercial advantage.

These risks exist to some extent with all foreign satellite services. However, they are more acute in the case of Starlink due to the company's technical dominance, Musk's influence in the US government, and his recent conduct.

Starlink operates the world's largest satellite constellation and offers the best internet speed and bandwidth. Being a part of SpaceX, Starlink can achieve a launch cadence that no other company or even government can presently match. This high launch cadence results in a large constellation, which, in turn, enhances coverage and performance. Competitors such as Amazon Leo (formerly Kuiper) constellation may challenge this dominance, but they are likely to take several years to catch up.

Elon Musk could further Starlink's commercial interests by influencing the US government to pressure India. He wields influence on US government policy in two ways. One is through his enduring relationship with US President Donald Trump, which has survived a brief public spat in 2025. Musk played a prominent role in Donald Trump's 2024 presidential campaign and later became the de facto leader of the Department of Government Efficiency (DOGE).[8] Two, SpaceX provides critical capabilities to US defence and space endeavours. It launches satellites for the National Reconnaissance Office (NRO), the US Space Force, and to support functions like missile warning and tracking.[9] SpaceX is also crucial to NASA's programmes to maintain a continuous human presence in LEO, and undertake the Artemis lunar exploration programme.[10]

Musk's influence is made more concerning by his conduct. Consider the case of Ukraine. Starlink started offering its services to Ukraine in February 2022 after the outbreak of hostilities with Russia. Ukraine soon became heavily dependent on Starlink for government and military communications. Despite this, Musk reportedly "restricted Starlink access multiple times" employing geofencing (remotely restricting service based on geographic location).[11] He also "denied the Ukrainian military's request to turn on Starlink near Crimea," directly impacting ongoing operations.[12]

The relationship also works in reverse. SpaceX depends on US government contracts and regulatory approvals for its commercial and national security launches, its spectrum allocations, and its orbital licensing. This gives the US government considerable leverage

over Musk and SpaceX. In a scenario where US strategic interests require it, Washington could pressure SpaceX to share data from Starlink's Indian operations, maintain or deny coverage over specific regions, or otherwise act in ways that serve American rather than Indian interests. Starlink's operator is ultimately subject to the authority and interests of a foreign government.

These concerns are compounded by statements from Musk, especially on his social media platform, X, previously known as Twitter. In 2025 he boasted that "my Starlink system is the backbone of the Ukrainian army. Their entire front line would collapse if I turned it off."[13] Two years earlier, he bragged about his access to data. "Between Tesla, Starlink & Twitter, I may have more real-time global economic data in one head than anyone ever," he posted.[14]

These concerns have proven to be more concrete over time. On 15 January 2026, Starlink updated its Global Privacy Policy to permit the use of customer data—including location information, user IP addresses, and what Starlink describes as "communication information, such as audio, electronic, or visual information"—to train machine learning and artificial intelligence models. The policy also permits sharing this data with unnamed "third-party collaborators" for AI training purposes.[15] Users are opted into data sharing by default. The policy update came two weeks before the announcement of SpaceX's merger with xAI, Musk's artificial intelligence company, which develops the Grok chatbot and owns the social media platform X. The merger gives xAI access to communication streams from over 10 million Starlink subscribers worldwide. Privacy advocates have warned that this arrangement creates new avenues for surveillance and data misuse.

Starlink's willingness to comply with government requests remains uncertain. During protests in Iran in 2022, Musk activated Starlink over the country for the first time, allowing protestors with Starlink terminals to bypass government restrictions in Internet access. In June 2025, Musk tweeted "The beams are on", barely a day after the commencement of the 12-Day Iran-Israel War.[16]

In December 2024, Indian security forces recovered Starlink equipment from a militant group in Manipur. Musk's reply on X was simply: "This is false. Starlink satellite beams are turned off over India."[17] The reality appears to be more complex. Because of the imperfections in geofencing, the devices may have worked in parts of the state bordering Myanmar.[18] About two weeks earlier, authorities in the Andaman and Nicobar Islands discovered smugglers were using Starlink devices.[19] The government approached Starlink and requested it to share details of the users of the devices as well as usage history. Starlink turned down the request.[20] Starlink cited data privacy laws and directed Indian authorities to channel their requests through US law enforcement or international protocols.

In summary, Starlink usage remains a risk for both large-scale retail markets and critical applications. Allowing widespread retail use of Starlink could result in loss of the state's ability to regulate internet access for reasons of internal security. Relying on Starlink for critical applications could mean the loss of connectivity when it is needed most, especially during a disaster, crisis, or conflict.

4 The Challenges of Blocking Illicit Starlink Usage

Starlink satellites are about sixty times closer to the Earth than geostationary systems, with each satellite's footprint being a lot smaller. LEO constellations like Starlink are inherently more difficult to block than a legacy GEO constellation such as Viasat. This is because:

1. The Starlink terminals use narrow-beam phased-antenna bands that form tight, electronically steered beams pointed at specific satellites.[21] The jammer will have to aim precisely into this constantly shifting beam. This requires near visual range physical proximity to the terminal.
2. At mid-latitudes, the constellation is a dense orbital mesh. Several dozen satellites are above the horizon at any moment, compared to the one or two fixed satellites in a GEO system. A terminal connects to one satellite at a time but can switch between them in milliseconds. This means jamming one link simply pushes the terminal to another satellite on a different orbital path. A GEO jammer can point at a fixed spot in the sky and hold; a Starlink jammer faces a constantly shifting target set that rotates every few minutes.
3. SpaceX can also adapt to new challenges and push over-the-air updates to terminals globally to counter jamming efforts.[22] For instance, in 2022, Musk posted on X that a software update had bypassed Russian jamming efforts within a few hours.[23]

4.1 Case Study: Ukraine

The earlier section discussed how Musk selectively restricted Ukraine's access to Starlink. Russia, for its part, attempted the opposite—to deny Ukraine the use of Starlink through electronic warfare. Its efforts had limited success.

Since 2022, Russia appears to have pursued multiple techniques to deny Ukraine use of Starlink:

1. **GPS Jamming**: Starlink terminals use GPS to self-determine their location and establish a connection with the most suitably positioned Starlink satellite. During

the course of the war, the Russians jammed GPS signals to degrade or prevent terminal connectivity. Since this jamming signal was a low-power signal that can be blocked by physical objects, Ukrainian soldiers placed terminals inside holes in the ground or behind barriers and thus avoided the jamming to a great degree.[24]

2. **Uplink Jamming**: Advanced Russian EW systems targeted uplinks from terminals on the ground to satellites. The most common target was the KU band between 10.9 to 14 gigahertz. Reports come from Bakhmut in early 2023 when Ukrainian drone operators reported severe uplink degradation.[25] The terminals could only send text messages and not support audio or video calls. Analysts assessed that these were due to Russian EW assets in action.

4.2 Case Study: Iran

An estimated 50,000 smuggled Starlink terminals were operating illegally in Iran at the beginning of 2026.[26] When protests that began in late December 2025 intensified in January 2026, authorities shut down terrestrial internet and Starlink became the de facto link for the protesters to the outside world.[27]

Iran responded with GPS jamming in major cities as well as RF jamming of the Ku-band and the Ka-band using mobile units.[28] These measures resulted in disruptions that were localised and temporary.

Authorities also reportedly employed Russian-made long-range jammers[29], drone surveillance to identify terminals on rooftops, and door-to-door raids to seize terminals.[30]

Furthermore, Iran made formal complaints to the International Telecommunications Union (ITU) claiming that Starlink was violating Iranian sovereignty.[31] The ITU Radio Regulation Board noted with 'grave concern' that Starlink had claimed terminals were not marketed, sold, or activated in Iran and not made an effort to disable all unauthorised terminals. The board noted that Starlink had demonstrated the capability to disable terminals en masse in other countries based on geographic location, but had chosen not to do so in Iran.[32]

5 India's Regulatory Response

In May 2025, the Department of Telecommunications released an Office Memorandum imposing additional security conditions on all operators holding a GMPCS license.[33] These conditions were issued over and above the existing security requirements in the

Unified License and apply to all satellite communication providers seeking to operate in India.

The conditions are extensive. The licensee must provide real-time monitoring facilities to security agencies and ensure that no user traffic to or from India is routed through any foreign gateway. The licensee is not permitted to route traffic through inter-satellite links (ISL) even in the event of a failure of its Indian gateways. All user traffic must pass through gateways located in India; direct terminal-to-terminal satellite communication is prohibited. The licensee must also support metadata collection by the DoT's Telecom Security Operation Centre and submit an undertaking to not copy or decrypt Indian telecom data outside the country.[34]

The conditions also address border security. Areas within 50 kilometres of international borders and coastal borders, including the Exclusive Economic Zone up to 200 nautical miles, are designated as special monitoring zones for user activity monitoring by law enforcement agencies. The licensee must restrict or deny services to individuals, groups, or areas during hostilities or as directed by law enforcement. Blocked websites must remain inaccessible through satellite services, location spoofing is prohibited, and user terminals must not connect to gateways outside Indian territory.[35]

Additionally, the conditions serve an industrial policy objective. The licensee must submit a phased manufacturing programme to indigenise at least 20 percent of the ground segment of its satellite network within five years of commercial launch. The licensee is also encouraged to integrate NavIC (India's indigenous satellite navigation system) in user terminals, with a transition plan for full implementation by 2029, though this remains on a best-effort basis.[36]

Also, India's space regulator, the Indian National Space Promotion and Authorisation Centre (IN-SPACe), rejected Starlink's application for its Gen 2 satellite constellation in January 2026. Gen 2 satellites incorporate direct-to-device (D2D) capability, which allows satellites to transmit signals directly to mobile phones without ground-based terminals. IN-SPACe granted clearance only for Starlink's Gen 1 system of 4,408 satellites, which supports conventional satellite broadband through user terminals and Indian gateways.[37] India currently has no regulatory framework for direct-to-device satellite services, and the Department of Telecommunications is still deliberating on a policy approach.

6 The Limits of Regulation

The effort at regulation faces fundamental enforceability challenges. Foremost of them being the ISL restriction. Starlink's architecture relies on inter-satellite links to route

traffic across its constellation. The conditions require that every packet originating from an Indian terminal travel up to a single satellite and come back directly to an Indian gateway without traveling through the orbital mesh. If an Indian gateway fails, the traffic cannot be rerouted—instead, it simply stops. This, however, negates the core resilience advantage of a satellite internet constellation like Starlink for Indian users. The regulatory authorities in India can inspect what happens at the Indian gateway but cannot independently verify what is happening in orbit. Inter-satellite links are optical laser communication pathways that allow satellites to exchange data directly without routing through ground stations. Whether a packet transited through an ISL before reaching the Indian gateway is not something ground-based monitoring can reliably detect.[38]

Some of the other conditions also rely on trust and self-certification rather than technical enforcement. The data handling condition needs a written undertaking not to copy or decrypt Indian telecom data outside India.[39] This self-certification mechanism is especially inadequate after Starlink's January 2026 privacy policy update, which explicitly authorises the use of customer data for AI model training and sharing with third parties. The NavIC integration is described as *best-effort* and has no penalty for non-compliance. Geofencing, which is a major condition that many security outcomes depend on, has already proven unreliable in practice as the Manipur and Andaman incidents showed. The Iran case is even more instructive: the ITU found that Starlink had the capability to disable terminals en masse but chose not to.

IN-SPACe's rejection of Starlink's Gen2 constellation can also prove challenging in the future as a regulatory question. IN-SPACe has said that it might reconsider the application.[40] The D2D technology can bypass the entire gateway-dependent architecture that India's current GMPCS conditions are built around. A phone will connect directly to a satellite and will not need an Indian gateway at all. The traffic could travel through the inter-satellite link to any gateway anywhere in the world. This makes India's data localisation and routing requirements irrelevant and ineffective.

If followed, the GMPCS does mitigate the data and surveillance risks outlined in the earlier section but they do not resolve the core problem which is that the operational control of the constellation remains with SpaceX. India's regulatory power is limited to post hoc penalties such as license revocation. It cannot compel Starlink to maintain services during a crisis if SpaceX decides not to, nor can it compel Starlink to hold services if SpaceX chooses to keep its satellites active. The turn-on and turn-off risks persist.

India also currently lacks an independent technical infrastructure to verify whether satellite operators are complying with these conditions. In late 2025, Communications Minister Jyotiraditya Scindia announced a ₹900 crore National SATCOM Monitoring

Facility. However, this facility has not yet been operationalised.[41]

7 Recommendations

GMPCS conditions represent a serious regulatory effort but are insufficient on their own because operational control of the constellation remains with SpaceX. India should therefore combine regulatory compliance with structural measures that reduce dependence. It should seek to limit the use of Starlink and other foreign satellite internet operators.

We recommend the following:

1. A government fund—Digital Bharat Nidhi (formerly USOF) for telecom connectivity in underserved areas already exists. Its corpus should be increased to fund the expansion of broadband internet into underserved areas.
2. India should prioritise satellite internet players with corporate structures that give India more leverage and control, something regulatory conditions alone cannot do. This could include prioritising providers that offer joint ventures with Indian entities, equity participation by Indian stakeholders, or those headquartered in jurisdictions where India has stronger bilateral enforcement mechanisms.
3. India can continue using Starlink for some applications such as disaster relief, while also subscribing to rival services to manage risks.
4. Much of the projected demand for satellite internet in India comes from rural and remote retail users in areas poorly served by terrestrial broadband. Allowing this demand to be met primarily by Starlink creates a structural dependency that will become hard to reverse. General retail use of foreign satellite internet services must therefore be discouraged as much as possible.
5. India should develop a regulatory framework for direct-to-device satellite technology proactively and not wait for its hand to be forced when the technology becomes widespread.
6. Operationalise the independent satcom monitoring facility for better enforcement of GMPCS.

Endnotes

1. Data sourced from Jonathan McDowell, Jonathan's Space Report, Link.

2. Ibid.

3. Tereza Pultarova, "Starlink Satellites: Facts, Tracking and Impact on Astronomy," *Space.com*, last modified December 18, 2025, Link.

4. "SpaceX Launches 3,000th Starlink Satellite in 2025 on Record-Setting 32nd Flight of Falcon 9 Booster," Spaceflight Now, December 8, 2025, Link.

5. Starlink Services, LLC, "Amended Application of Starlink Services, LLC," filing before the Public Utility Commission of Oregon, Federal Communications Commission docket (RDOF), 2021, Link.

6. Alex Sherman, " 'Muskonomy' Shakeup: SpaceX Valuation Approaches Tesla's After Merger with xAI," CNBC, February 3, 2026, Link.

7. Alex Sherman, " 'Muskonomy' Shakeup: SpaceX Valuation Approaches Tesla's After Merger with xAI," CNBC, February 3, 2026, Link.

8. Bobby Allyn and Suzanne Noh, "From Bromance to Breakup: How Elon Musk and Donald Trump Blew Up," NPR, June 5, 2025, Link.

9. SSC Public Affairs, "Space Systems Command Awards Task Orders to Launch Missile Warning and Missile Tracking Space," Space Systems Command, January 9, 2026, Link.

10. Aditya Ramanathan, "Human Spaceflight: Indian Goals & Global Ambitions," Takshashila Discussion Document No. 2023-13, November 2023, The Takshashila Institution, Link.

11. Adam Satariano, Scott Reinhard, Christina Hinshaw, and Jeremy White, "Elon Musk's Unmatched Power in the Stars," *New York Times*, July 28, 2023, Link.

12. ibid

13. Elon Musk (@elonmusk), "I literally challenged Putin to one on one physical combat over Ukraine and my Starlink system is the backbone of the Ukrainian army. Their entire front line would collapse if I turned it off. What I am sickened by is years of slaughter in a stalemate that Ukraine will inevitably lose. Anyone who really cares, really thinks and really understands wants the meat grinder to stop. PEACE NOW!!" X, March 9, 2025, Link.

14. Elon Musk (@elonmusk), "Between Tesla, Starlink & Twitter, I may have more real-time global economic data in one head than anyone ever," X, April 30, 2023, Link.

15. Starlink Services, LLC, "Global Privacy Policy," updated January 15, 2026, Link.

16. The Conversation, "In the Sky over Iran, Elon Musk and Starlink Step into Geopolitics — Not for the First Time," June 26, 2025, Link.

17. Elon Musk (@elonmusk), reply to @i_am_dipshikha, "This is false. Starlink satellite beams are turned off over India," *X*, December 17, 2024, Link.

18. Kamya Pandey, "Report: Government Investigates Starlink Devices Found in Manipur Militant Camp," *MediaNama*, May 8, 2025, Link.

19. Kamya Pandey, "Smugglers Navigate $4.25B Meth Shipment to India Using Starlink Devices, Police Probe Usage History," *MediaNama*, December 4, 2024, Link.

20. ET Online, "Starlink Under Govt Scrutiny after Company Refuses to Reveal Details on Who Used Its Satcom Devices in India," *Economic Times*, January 3, 2025, Link.

21. Curtis Arnold, "An Overview of How Starlink's Phased Array Antenna (Dishy) Works," LinkedIn Pulse, Link.

22. SpaceNews, "SpaceX Shifts Resources to Cybersecurity to Address Starlink Jamming," Link.

23. Space.com, "Elon Musk: SpaceX's Starlink Defeated Ukraine Cyberattack," Link.

24. Defense One, "Using Starlink Paints a Target on Ukrainian Troops," March 2023, Link.

25. Clara Kaluderovic, "The Coming Compute War in Ukraine," Atlantic Council, March 16, 2026, Link.

26. "Iran's Crackdown on Starlink Sellers Hits Rare Link to Internet," Bloomberg, March 31, 2026, Link.

27. Amnesty International, "Iran Internet Shutdown Hides Violations in Escalating Protests," January 8, 2026, Link.

28. Euronews, "Iran could be blocking Starlink during internet blackout with methods similar to Russia," January 2026, Link.

29. Ibid.

30. Sinha, "How Iran Neutralised Starlink."

31. International Telecommunication Union, Radio Regulation Board, Link.

32. ibid

33. Department of Telecommunications, Office Memorandum on Security Conditions for GMPCS License, May 5, 2025. Analysed in: Aprajita Rana et al., "Update – Security Conditions under the GMPCS License," AZB & Partners, May 29, 2025, Link.

34. Ibid.

35. Ibid.

36. Ibid

37. "India Rejects Elon Musk's Gen 2 Starlink Application," *Zee News*, January 29, 2026, Link. "Starlink Will Need Fresh Approval from IN-SPACe for D2D Connectivity," *Inc42*, January 27, 2026, Link.

38. Ashwin Prasad, "Satellite Internet Explained: How It Works and Why It Matters," Takshashila Discussion Document No. 2025-09, Version 1.0, April 2025, The Takshashila Institution, pp. 19–23.

39. AZB & Partners, "Update – Security Conditions under the GMPCS License."

40. "Starlink Internet Won't Connect to Indian Phones Anytime Soon; Here's Why," Outlook Business, January 27, 2026, Link.

41. "Minister Scindia announces groundbreaking policy reforms and projects to secure India's leadership in satellite communication," PIB, October 8, 2025, Link.

The Takshashila Institution is an independent centre for research and education in public policy. It is a non-partisan, non-profit organisation that advocates the values of freedom, openness, tolerance, pluralism, and responsible citizenship. It seeks to transform India through better public policies, bridging the governance gap by developing better public servants, civil society leaders, professionals, and informed citizens.

Takshashila creates change by connecting good people, to good ideas and good networks. It produces independent policy research in a number of areas of governance, it grooms civic leaders through its online education programmes and engages in public discourse through its publications and digital media.