

DR. SUBRAMANIAN SWAMY Ph.D. (Harvard)
Cabinet Minister for Commerce, Law & Justice (1990-91)
Chairman (with Cabinet rank), Commission on Labour
Standards and International Trade (1994-96)
Former Professor of Economics, Indian Institute of
Technology, Delhi & Faculty, Harvard University
Member of Parliament (Six Terms 1974-2022)



सत्यमेव जयते

Res.: A-77, Nizamuddin East, New Delhi-110013
Phone: +91 11 35839141
+91 11 35803155
E-mail: swamy39@gmail.com
swamy@post.harvard.edu

22.10.2026

To,

Mr. Amit Anilchandra Shah

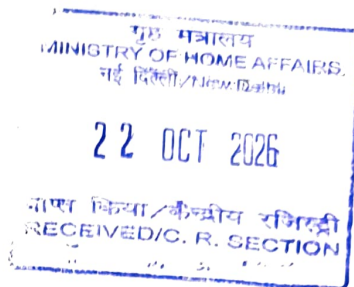
The Hon'ble Union Home Minister and

Minister of Co-operation of India

Ministry of Home Affairs

Government of India

North Block, New Delhi – 110001



**SUBJECT: REPRESENTATION SEEKING AN URGENT NATIONAL
SECURITY REVIEW AND SUSPENSION OF STARLINK'S APPROVAL
AND OPERATIONAL AUTHORISATION IN INDIA PENDING
SATISFACTORY ASSESSMENT OF SECURITY CONCERNS**

Dear Amit Bhai,

I am writing to express my serious concern regarding the national security implications arising from the proposed introduction and operation of Starlink's satellite-based internet services in India. In view of the strategic significance of communications infrastructure and the potential implications of foreign-controlled satellite networks, I urge the Ministry of Home Affairs to undertake an immediate and comprehensive security review and ensure that national security is not compromised in the pursuit of technological advancement or commercial interests.

1. National Security and Strategic Autonomy: Satellite-based internet connectivity has the potential to improve communications, particularly in remote and underserved areas. However, the introduction of such services must be assessed not merely from the standpoint of technological advancement or commercial convenience, but primarily through the lens of national security, sovereignty, strategic autonomy and the protection of sensitive information.

1.1. The operation of a satellite internet network raises important questions concerning foreign control over critical communications infrastructure, the routing and storage of sensitive data, access to network-related information by foreign

entities, the effectiveness of lawful interception mechanisms, cyber vulnerabilities and the ability of Indian authorities to exercise effective oversight in accordance with Indian law.

2. **Potential Vulnerabilities Requiring Examination:** Particular attention must be given to the implications of such networks for communications associated with defence establishments, strategic installations, government institutions and other locations of national importance. The competent authorities should examine whether adequate technical and legal safeguards exist to prevent unauthorised access, external interference, disruption of services and the exploitation of network vulnerabilities.

2.1. The Government must also assess the extent to which Indian authorities would retain effective regulatory control, access to information necessary for lawful investigations, and the ability to issue and enforce directions in circumstances involving national security or public emergency.

2.2. The possibility of foreign jurisdictional pressures, dependence on infrastructure operated or controlled by foreign entities, and the interruption or restriction of essential communications services must be evaluated before the network becomes operationally significant.

2.3. These concerns are raised as matters warranting rigorous examination by the competent authorities and not as a presumption that any particular security breach has already occurred.

3. **Need for an Independent and Comprehensive Security Assessment:** It is imperative that the relevant security implications be independently examined before any approval or operational authorisation is treated as conclusive. Such an assessment should involve the Ministry of Home Affairs, the Intelligence Bureau, the Ministry of Defence, the Department of Telecommunications, the Ministry of Electronics and Information Technology and other competent agencies, as appropriate.

3.1. The assessment should specifically examine:

- a) the architecture and control of the satellite communications network and its associated ground infrastructure;
- b) the collection, routing, processing, storage and jurisdictional accessibility of user and network data;
- c) the adequacy of encryption, key management, cybersecurity safeguards and protection against unauthorised access;

- d) the ability of Indian authorities to enforce applicable lawful interception requirements and other legally binding directions;
- e) the protection of sensitive communications and strategic installations against unauthorised access or interference;
- f) the risks arising from dependence on a foreign-controlled communications network, including possible disruption or restriction of services during a national security emergency; and
- g) the adequacy of security audits, incident reporting, regulatory inspection, emergency response mechanisms and enforceable compliance conditions.

4. Precautionary Approach and Suspension Pending Review: Where critical communications infrastructure is concerned, the absence of a publicly established security incident cannot, by itself, be treated as conclusive proof that all material risks have been addressed. A prior, independent and technically informed assessment is necessary to determine whether the proposed operations are compatible with India's security requirements.

- 4.1. Once a foreign-controlled communications network becomes deeply integrated into the country's digital ecosystem, addressing vulnerabilities retrospectively may prove considerably more difficult. It is therefore prudent to adopt a precautionary approach and resolve all material security concerns before permitting further implementation or expansion.
- 4.2. Accordingly, I urge the Ministry of Home Affairs to examine whether any approval, licence or operational authorisation granted to Starlink should be suspended, restricted or kept in abeyance, pending completion of the security assessment and satisfactory resolution of all material concerns, subject to the applicable statutory framework and the powers of the competent authorities.
- 4.3. The Government should also examine whether existing authorisation conditions adequately provide for security audits, regulatory inspection, compliance with lawful directions, incident reporting, continuity of essential services and suspension or revocation in the event of a material security concern or breach of applicable conditions. Any identified deficiencies should be

addressed before the services are permitted to expand or become operationally integral to critical sectors.

5. In view of the foregoing, I respectfully request your personal intervention and urge the Ministry of Home Affairs to:

- (i) Direct an urgent, comprehensive and independent assessment of the national security, intelligence, cybersecurity and strategic implications of Starlink's proposed or approved operations in India.
- (ii) Coordinate with the competent intelligence, defence, telecommunications and cybersecurity authorities and obtain a consolidated assessment of the risks and the adequacy of existing safeguards.
- (iii) Recommend that the relevant approval, licence or operational authorisation be kept in abeyance, or appropriately suspended or restricted, pending completion of the assessment and satisfactory resolution of material security concerns, to the extent permissible under law.
- (iv) Ensure that adequate and enforceable safeguards are in place to protect sensitive government communications, defence establishments, strategic assets and other locations of national importance.
- (v) Require an examination of the network's technical architecture, data handling practices, cybersecurity safeguards, lawful interception capabilities and the extent of effective Indian governmental oversight.
- (vi) Ensure that any permission ultimately granted or continued is subject to strict, enforceable and independently verifiable conditions under Indian law, together with effective mechanisms for monitoring compliance and responding to security incidents.
- (vii) Take such further action as may be considered appropriate under the applicable law to ensure that India's national security interests remain paramount in all decisions concerning Starlink's operations.

6. I wish to emphasise that this representation is not an objection to technological progress as such. It is, rather, an appeal to ensure that technological advancement proceeds in a manner consistent with India's sovereignty, strategic autonomy and national security.

7. No commercial interest, however substantial, should be permitted to override the Government's paramount responsibility to protect the nation.

The security implications of critical communications infrastructure must be assessed in advance, with appropriate safeguards established before material risks are allowed to arise.

8. I therefore request your urgent intervention to ensure that no further implementation or operationalisation of Starlink's services is permitted, and that any existing authorisation is reviewed for suspension or restriction in accordance with law, until the competent authorities are satisfied that India's national security interests are adequately protected.
9. I would appreciate an appropriate response indicating the action taken or proposed to be taken on this representation.
10. For any clarification or assistance that may be required in relation to this representation, your office may kindly contact my associate, **Mr. Satya Sabharwal, Advocate, at 9999034034.**

Yours sincerely,

Warm Regards!



Dr. Subramanian Swamy