Starlink Installation and Operation in high-threat environments

Introduction

Starlink can deliver internet service in areas where ground infrastructure is unavailable, unreliable, or untrustworthy. When using Starlink in high-threat environments, additional considerations should be made regarding the terminal installation's location and operation. This document provides general guidelines for reducing the ability of bad actors to detect, disrupt, or deny access to Starlink service. These guidelines are based upon public documentation. No empirical measurements or tests have been completed to validate these guidelines, and this material is provided "as is." The author assumes no responsibility for any typographical, technical, or other inaccuracies in this document. The author of this document does not represent SpaceX or Starlink in any way.

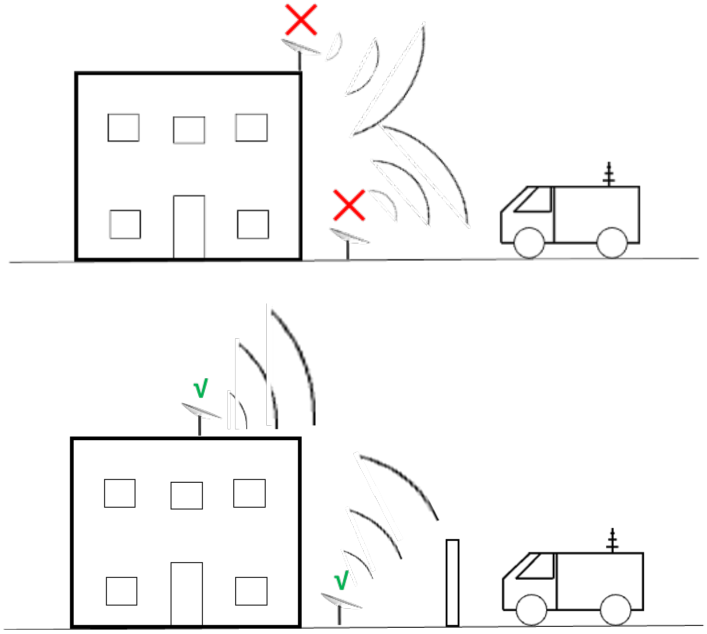
Background

The Starlink terminal employs phased-array technology to electronically direct transmissions to non-geostationary orbit (NGSO) satellites overhead. A general understanding of the terminal and its operation can be obtained from the public FCC filing. During normal operation, the Starlink terminal generates a beam of radio frequency (RF) energy in the direction of the satellites as they move across the sky. In addition to generating the intended or main beam, additional sidelobes are generated. Both the main beam and sidelobes can be detected by appropriate radio frequency (RF) detection equipment. Once detected, additional techniques can be used to geolocate a specific Starlink terminal. The Starlink service was not designed to offer the low probability of intercept (LPI) nor low probability of detection (LPD) typical of militarized radio waveforms. However, aggressive radio spectrum efficiency techniques in use by Starlink indirectly provide a decent level of security inherent within the architecture.

Recommendations

Operation of Starlink within a geographic area can be easily determined by detecting RF energy from satellites overhead. Geolocation of a specific Starlink terminal is more complicated, requiring imagery analysis or RF direction-finding equipment. The recommendations below are designed to mitigate, but not eliminate, geolocating a specific Starlink terminal.

1. **Install high with setback** – After powering up, the Starlink terminal will tilt in the primary direction of transmission. If possible, install the Starlink terminal in a position from which physical structures or vegetation naturally block horizontal RF signals as shown in the diagrams below.



2. **Use the Starlink app** – Use the "visibility" feature of the Starlink app to confirm the service will not be obstructed, while also positioning the Starlink near natural or constructed obstructions.
3. **Power off when not in use** – While powered on, the Starlink terminal will transmit RF energy even when the internet is not in use. Powering off the terminal will eliminate all transmissions.
4. **Ditch the supplied WiFi hardware** – Every piece of WiFi equipment transmits a unique address that provides indication of the equipment manufacturer. Use of a non-Starlink WiFi router common in the region or country of use will ensure the WiFi signal alone will not be used to detect the use of Starlink.
5. **Cover or remove during daylight hours** – During daylight hours, aircraft or drone imagery may be used to locate installed terminals.
6. **Consider going mobile** – A terminal in motion will generally be more difficult to geolocate but this must be weighed against the level of threat within the area of travel.