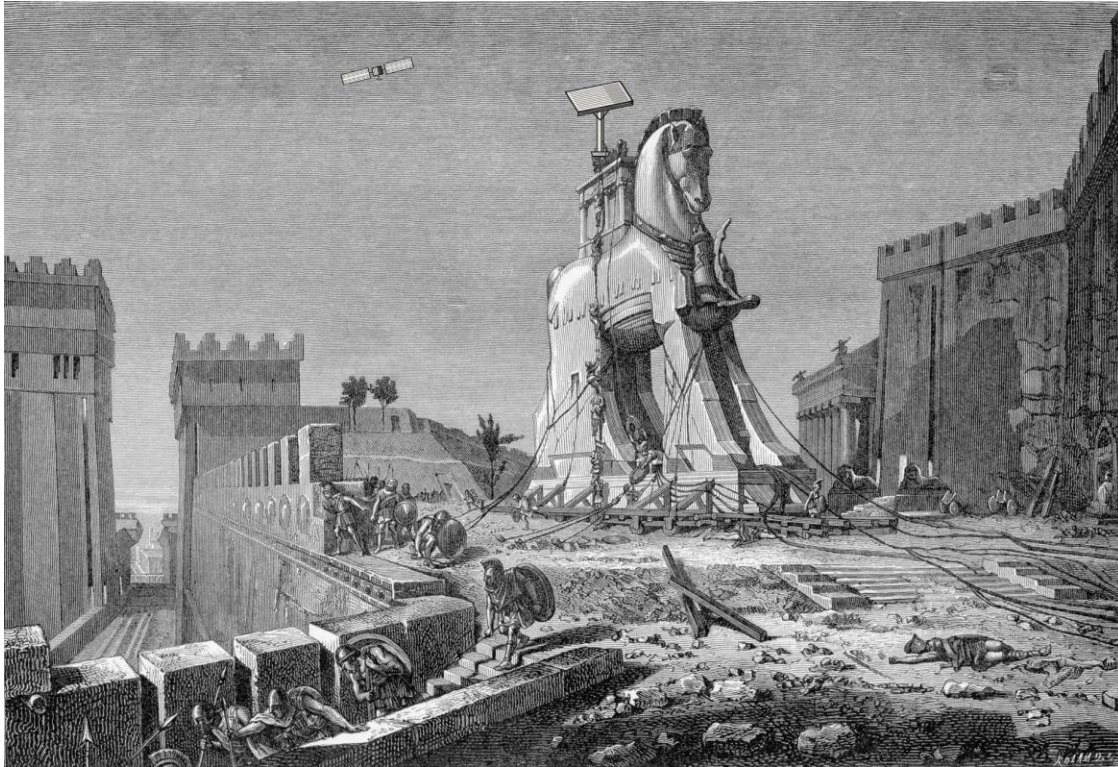


Starlink: Technology, Control, Military Use and Risk

An investigation



Prepared by: Mike

Research assistant: Claude (AI model, Anthropic)

Version: Draft academic paper for review, 14 October 2026

Status: Evidence current to October 2026. Subject to revision.

Contents

Section	Page
Abstract	3
Executive summary	3
Introduction	4
1. What is Starlink?	5
2. The technology	7
3. An independent “internet of the sky”?	9
3.1 Can Starlink operate independently of a ground connection?	9
3.2 Could Starlink become an “internet of the skies”, separate from the ground internet?	11
4. Independent computing power	13
5. How Starlink is controlled	14
6. Switching service on and off	16
6.1 How service is switched on and off	16
6.2 Protection against an idiosyncratic turn-off by Musk or the US President	16
7. Military and government use	18
7.1 Starshield: the military and government parts of Starlink	18
7.2 Weapons in space and the Starlink connection	20
8. Links between Starlink and Grok	20
9. History of Starlink in conflict situations	22
10. Potential dangers and their impact	24
10.1 The dangers, in order of severity	24
10.2 Assessments of the consequences of a turn-off	25
10.3 Impact assessment: a Starlink turn-off in Ukraine	27
10.4 Could an outside body get into the network?	29
10.5 The danger of AI independently infecting the network	31
10.6 Worst-case scenario: an AI takes control of the Starlink network	33
11. Actions to reduce the dangers, in order of urgency	35
12. Points for discussion	37
12.1 Lessons from the Trojan horse	37
12.2 Lessons from Dr Strangelove, including weapons in space	38
12.3 Other risks	40
13. Appendix: unresolved issues	41
References	44

Abstract

Starlink, operated by SpaceX, has become the largest satellite network ever built: about 11,100 satellites in orbit and more than 12 million customers in over 160 countries by late 2026. It is now central to Ukraine's defence, to US military communications and to connectivity in places that terrestrial networks do not reach. This paper investigates what Starlink is, how its technology works, how it is controlled and switched on and off by area, its military and government variants (Starshield), its links to the AI company xAI and its chatbot Grok, and its history in conflicts from Ukraine to Iran, Sudan, Gaza and Yemen. Evidence is drawn from regulatory filings, government statements, academic research and journalism, and each finding is rated as Confirmed, Reported or Unverified.

The paper finds that Starlink is **not an independent "internet of the sky"**: all internet traffic leaves through SpaceX-controlled ground sites, and control rests centrally with SpaceX and ultimately with one individual who holds about 82% of its voting power. That control has repeatedly been used, or reportedly used, to shape events in conflicts. The greatest danger identified is **structural**: dependence on a single point of control and failure, closely entangled with one government. Risks from cyber attack and from artificial intelligence are lower today but rising, as SpaceX integrates its AI business and plans orbital computing. The paper ranks these dangers by severity, sets out actions by urgency, and offers two cultural lenses, the Trojan horse and *Dr Strangelove*, for discussion.

Executive summary

Key findings

#	Finding	Confidence	Section
1	Starlink is the world's largest satellite network, owned by SpaceX, which listed on Nasdaq in June 2026. Elon Musk holds about 82% of the votes. SpaceX has owned xAI (Grok and X) since February 2026	High	1
2	The network combines low-orbit satellites, a mesh of over 13,000 laser links, phased-array dishes, direct-to-phone service and a SpaceX-run ground network	High	2
3	It is not independent of the ground internet. All internet traffic exits through SpaceX ground sites. A separate "internet of the skies" is not a realistic near-term prospect, but a more self-contained, single-company network is emerging	High	3
4	Satellites have substantial on-board computing and act autonomously for tasks such as collision avoidance, but remain commanded from the ground. Large-scale computing in orbit (Starmind) is planned but unproven	Medium-high	4
5	SpaceX controls the network centrally, at the level of satellites, individual terminals, approved lists, geographic areas, countries and permitted uses	High	5
6	Service can be switched on or off for one terminal, a region or a country, without anything on the ground there. Protection against an idiosyncratic turn-off is weak and not publicly guaranteed	High	6
7	SpaceX's military business, Starshield, supplies spy satellites, secure communications and much of the Golden Dome missile-defence space layer, possibly including interceptors	Medium-high	7
8	Starlink and Grok are linked by ownership, staff, customer support, a default AI-training data policy and orbital-computing plans. No evidence that Grok controls the network	Medium	8
9	Starlink has shaped conflicts since 2022: switched on (Ukraine, Iran), restricted or cut off (Crimea, reportedly Kherson, Sudan, Myanmar, Russian forces), and spread through	High	9

	black markets		
10	The most severe danger is concentration and dependence, followed by entanglement with one government and accidental failure. Cyber and AI risks are lower today but rising	Medium (judgement)	10

Most urgent actions

1. Critical users (militaries, emergency services, hospitals, energy) should maintain tested fallback communications.
2. Governments should disclose, or at least secure, service-continuity terms in their Starlink and Starshield contracts.
3. Regulators should examine Starlink's January 2026 AI data-training policy and whether data reaches Grok.
4. Independent security audit of Starlink's ground and software-update systems.

See section 11 for the full list.

Introduction

Objective

To undertake an extensive investigation into Starlink and to record the findings in a professionally structured document. The investigation is to be finalised in two forms: this detailed academic-style paper with full references, and a shorter, all-reader magazine-style article.

Research questions

#	Question	Section
1	What is Starlink?	1
2	What technologies does Starlink use?	2
3	Does Starlink create an independent "internet of the sky"?	3
4	Do Starlink satellites have independent computing power?	4
5	How is Starlink controlled?	5
6	How is Starlink switched on and off in different areas?	6
7	Does Starlink provide connections to support military operations?	7
8	Is Starlink connected to, or controlled by, Grok?	8
9	What is the history of Starlink's use in conflict situations?	9
10	What are the potential dangers, and how severe could their impact be?	10
11	What actions are needed to reduce the dangers, in order of urgency?	11
12	Points for discussion: lessons from the Trojan horse, <i>Dr Strangelove</i> (including weapons in space) and other risks	12
13	Unresolved issues	13 (Appendix)

Scope

In scope: the Starlink constellation, ground infrastructure and terminals; control and switching of service; military and government use, including Starshield; links to xAI and Grok; use in conflicts; and dangers and mitigations.

Out of scope: consumer pricing and plan comparisons, and detailed comparison with competing systems except where relevant to dependence and alternatives.

Method and evidence ratings

Each line of enquiry was researched separately between 12 and 13 October 2026 and recorded with its sources. Research, drafting and checking were carried out with the assistance of Claude, an AI model made by Anthropic, working under the author's direction. Every factual claim is linked to a cited source so that it can be checked independently. Every factual claim is rated:

- **Confirmed:** a primary source (for example a regulatory filing or official statement) or several independent credible sources.
- **Reported:** one credible source, or several that may share an origin.
- **Unverified:** a claim, a reasonable inference, or speculation.

Interpretive sections (10–12) are labelled as the investigation's own judgement and carry confidence levels (high, medium or low). Where sources disagree, both are recorded. Sections 10.6 and 12 contain hypothetical scenarios and cultural comparisons intended to support discussion, not forecasts.

Sources

Sources include SpaceX's SEC registration statement (Form S-1), US government notices, the Ukrainian government, peer-reviewed and preprint academic research, independent evaluators of AI risk, and established news organisations. Company statements, social-media posts and vendor white papers are used with caution and labelled. All sources are listed, numbered, in the References.

Illustration

Title-page illustration: a nineteenth-century wood engraving of the Trojan horse being brought into Troy, modified for this paper to add a satellite terminal and a satellite.

Limitations

Some important matters cannot be verified from public sources: the terms of military contracts, the technical method of geofencing, SpaceX's internal recovery procedures, and whether customer data is used to train Grok. Several conflict-zone claims rest on anonymous sourcing and have been denied. These are collected in the Appendix (section 13).

1. What is Starlink?

Researched 12 October 2026.

Summary

Starlink is a satellite internet service run by SpaceX. It uses a very large constellation of satellites in low Earth orbit (around 550 km up) to provide broadband to homes, businesses, ships, aircraft, governments and, more recently, ordinary mobile phones. It is now the largest satellite network ever built: about 11,100 satellites were in orbit as of

October 2026, and it had more than 12 million customers in over 160 countries and territories by mid-2026. Starlink is SpaceX's main source of revenue.

Since February 2026, SpaceX has also owned xAI, the company behind **Grok** and the social network **X**. SpaceX became a public company in June 2026, and Elon Musk controls about 82% of the votes. This changes the starting point for section 8: Starlink and Grok are now owned by the same company.

Ownership and business structure

Finding	Rating	Source
Starlink is operated by Space Exploration Technologies Corp. (SpaceX), a Texas corporation	Confirmed	[1]
SpaceX acquired xAI Holdings Corp. (xAI, owner of Grok and X) with effect from 2 February 2026. xAI had already acquired X (formerly Twitter) on 28 March 2025	Confirmed	[1], [2]
In May 2026 Musk announced xAI would stop being a separate company, with Grok and X becoming SpaceX's AI division. In April 2026 a former Starlink vice president, Michael Nicolls, became president of xAI	Reported	[2]
SpaceX listed on Nasdaq as SPCX on 12 June 2026 at \$135 a share, valuing it at about \$1.77 trillion	Confirmed	[3], [4]
Musk is founder, CEO, CTO and Chairman. He owns about 42% of the shares but holds about 82% of the voting power through Class B shares (10 votes each), so SpaceX is a "controlled company"	Confirmed (structure) / Reported (percentages)	[1], [3]
The Connectivity segment, "primarily driven by Starlink", earned \$11.4 billion in 2025, about 61% of SpaceX's total revenue, and about 69% in Q1 2026	Confirmed (figures) / own calculation (percentages)	[1]

History and growth

Date	Event	Rating	Source
January 2015	Starlink announced, with regulatory filings for about 4,000 satellites	Confirmed	[5]
February 2018	Two test satellites, TinTin A and B, launched	Confirmed	[5]
23 May 2019	First batch of 60 operational satellites launched	Confirmed	[5], [6]
Late 2020	Public beta service begins	Reported (to check against primary source)	—
February 2023	Start of V2 Mini satellites (larger, with upgraded antennas and argon thrusters)	Confirmed	[5]
31 March 2026	About 9,600 broadband and mobile satellites in orbit; 10.3 million subscribers in 164 countries, territories and markets	Confirmed	[1]
June 2026	SpaceX reports more than 12 million active customers in 160+ countries	Reported (company statement on X)	[7]
11 October 2026	11,137 Starlink satellites in orbit (11,123 working); 12,988 launched in total, about 1,850 already deorbited	Reported (independent tracker)	[6]

Notes

- Satellites last about five years and are then deliberately deorbited and replaced, so the network is constantly being refreshed. [5]
- The FCC has authorised 12,000 satellites, and SpaceX has filed internationally for up to about 30,000 more (around 42,000 in total). [5]

Who uses it

- **Consumers and businesses:** fixed broadband, especially in rural and poorly served areas. [1]
- **Maritime and aviation:** ships and airline Wi-Fi. [1], [8]
- **Mobile phones (direct-to-cell):** about 650 dedicated mobile satellites serving about 7.4 million devices a month in around 30 countries, through partnerships with about 30 mobile networks (as of March 2026). [1]
- **Governments:** public services, humanitarian and disaster response. **Starshield** is a separate secure network built from Starlink technology for US government and national security customers (covered further in 7). [1]

Where it operates and where it doesn't

Status	Countries (examples)	Rating	Source
Available	Most of the Americas and Europe (including the UK); Ukraine, but with Crimea and occupied Donbas geofenced out; Australia, New Zealand, Japan, Indonesia, Philippines; about 27 African markets including Nigeria	Reported	[8]
Pending or uncertain	India: reports conflict. One source says final approval came in Q1 2026, but June 2026 reporting says only a letter of intent was in place and security agencies were withholding clearance, which Starlink denies. Also Pakistan, South Africa, Saudi Arabia, Vietnam (licensed February 2026)	Reported, conflicting	[8], [9]
Banned or blocked	China (including Hong Kong and Macao), Russia, Belarus, North Korea, Afghanistan, Syria, Cuba (sanctions), Iran (possession criminalised)	Reported	[8]

Points to follow up

- Starlink terminals are reportedly used in places where it is not licensed (for example Iran). This links to how service is switched on and off (5) and use in conflict (9).
- India's concern was reportedly about whether it could control a US operator during a conflict. This is relevant to 5.
- The geofencing of occupied parts of Ukraine is direct evidence that Starlink controls service by area (5, 9).
- Common ownership of Starlink and Grok is now confirmed. Section 8 should look at whether there is any *operational* link, not just shared ownership. The S-1 describes plans for Starlink to connect future "orbital AI compute" satellites to users. [1]

2. The technology

Researched 12 October 2026.

Summary

Starlink has four main parts: **satellites** in low Earth orbit, **laser links** that join the satellites into a mesh in space, **user terminals** (the dishes, plus ordinary mobile phones for direct-to-cell), and a **ground network** of gateway stations and internet connection points.

A typical connection goes like this. The dish sends to a satellite by radio, the data may hop between satellites by laser, then it comes down to a ground station and passes into SpaceX's own network before reaching the public internet. The lasers mean traffic can cross oceans and remote areas without a ground station nearby, but **all internet traffic still has to come down to a SpaceX ground site** at some point.

Each satellite carries a lot of computing power. It runs Linux and **avoids collisions on its own, with no ground command needed** (about 355,000 manoeuvres in the year to May 2026). The newest V3 satellites first reached orbit on 28 September 2026. SpaceX has also

asked the FCC for permission for up to one million “orbital data centre” satellites for AI computing. That has not been approved.

Satellites

Finding	Rating	Source
Generations: V1 (about 260 kg) and V1.5 from 2019; V2 Mini from February 2023 (laser links, argon thrusters, upgraded antennas, launched on Falcon 9); V3 built for launch on Starship	Confirmed	[5], [10]
First V3 satellites: 26 deployed on Starship Flight 14, 28 September 2026. Each one is rated at about 1 Tbps download and 160 Gbps upload, roughly 10 times the download and 22 times the upload of a V2 satellite	Reported	[10], [11]
Orbit: mostly around 550 km, much lower than geostationary satellites at about 36,000 km, which is why delay (latency) is low	Confirmed	[5]
Lifespan about five years, then deliberately deorbited to burn up	Confirmed	[5]
FCC Gen2 authorisation rose to 15,000 satellites in January 2026	Reported	[12]
Total network capacity was nearly 450 Tbps in mid-2025, with over 5 Tbps added each week	Reported (company figures)	[13]

Laser links: the mesh in space

Finding	Rating	Source
Each V2 Mini satellite has three laser links to other satellites	Reported	[12]
Each laser link runs at up to 100–200 Gbps, over distances up to about 5,400 km	Reported (company presentation)	[12], [14]
In January 2024 the mesh had over 9,000 lasers carrying about 42 million GB (42 PB) a day, with 99.99% uptime from fast rerouting (SpaceX engineer at SPIE Photonics West)	Reported	[14]
SpaceX’s 2025 Progress Report describes a “petabit-class” mesh with more than 13,000 two-way laser links	Reported	[12]
Lasers carry traffic between satellites, but it still has to come down to a ground gateway or authorised connection point to reach the internet. They reduce dependence on ground stations without removing it	Reported (two independent sources agree)	[12], [15]

User terminals

Finding	Rating	Source
Dishes use a flat phased-array antenna , which steers its beam electronically to track satellites as they cross the sky	Confirmed (widely documented)	[15]
Dish to satellite uses the Ku band . Satellite to ground station uses the Ka band , and SpaceX is adding E-band at gateways for more capacity	Reported	[15], [16]
Terminal types include the Standard dish, the small portable Mini, and higher-power Enterprise/maritime/aviation versions	Unverified (no source yet; to confirm from Starlink’s specification pages)	—
Typical US performance in mid-2025: median peak-hour download 200 Mbps, latency about 26 ms (target 20 ms)	Reported (company figures)	[13]

Ground network

Finding	Rating	Source
Gateways are ground stations that link satellites to fibre. The US alone had over 100 gateway sites by mid-2025	Reported	[13], [16]
Points of presence (PoPs) are SpaceX’s connection points to the internet. A late-2024 academic study found about 37 PoPs worldwide, linked by SpaceX’s own	Reported (academic)	[15]

backbone

Each user's traffic is tunnelled to an assigned "home" PoP before it reaches the public internet. Some PoPs serve many countries: Frankfurt served users in 36 regions across Europe, Asia and Africa

Reported (academic) [15]

Gateways need local licences. Examples include E-band gateway licences from Ofcom in the UK (2025) and Vietnam's first four licensed gateways (2026)

Reported (headlines only, articles not yet read) [32], [33]

Direct-to-cell (satellite to ordinary phone)

Finding	Rating	Source
Direct-to-cell satellites carry an eNodeB modem , the same equipment as a mobile phone mast, so the satellite acts as a "cell tower in space". It works with standard, unmodified LTE phones for text, voice, data and IoT, using laser links to carry traffic back	Confirmed (Starlink)	[17]
About 650 dedicated mobile satellites, about 7.4 million devices a month, around 30 mobile network partners including T-Mobile (March 2026)	Confirmed	[1]
SpaceX bought EchoStar's AWS-4 and H-Block spectrum for \$17 billion, giving it its own 50 MHz block. It plans to compete directly as a mobile carrier with next-generation direct-to-cell satellites	Reported	[18]

On-board computing

Covered in section 4.

3. An independent "internet of the sky"?

3.1 Can Starlink operate independently of a ground connection?

Researched 12 October 2026. Original question 3: does Starlink create an independent "internet of the sky"?

Short answer

It depends what "independent" means. There are four different questions:

Question	Answer	Rating
Can Starlink serve an area with no local ground station ?	Yes. Laser links carry traffic thousands of km through space to a ground station elsewhere. This is how it serves ships mid-ocean, remote regions, and countries where SpaceX has no gateways	Confirmed
Can it give internet access with no ground connection anywhere ?	No. The internet is on the ground. All commercial traffic is tunnelled to a SpaceX point of presence (PoP) on the ground before reaching the public internet	Reported (academic and industry sources agree)
Could it run a closed network in space , user to user without touching the ground?	Technically plausible, but not offered commercially. The laser mesh could do it, but commercial traffic is sent to the user's home PoP, so even two users in the same town are routed via the ground. The military MILNET system is designed to move data across the laser mesh and reduce reliance on ground stations	Unverified (commercial) / Reported (military design)
Can the satellites keep running without ground control ?	Partly, and only for a while. They steer beams and avoid collisions on their own, but they are commanded, updated and managed from the ground. They also last only about five years, so without new launches the network would shrink	Reported (autonomy) / own inference (long term)

The detail

1. Ground stations don't need to be local. Each satellite has three laser links at up to 100–200 Gbps, over distances up to about 5,400 km [12], [14]. Traffic from a user can hop across several satellites before coming down at a gateway in another country. This is what lets Starlink work in places where it has no ground stations, and is likely how terminals reportedly work in countries where it is not licensed, such as Iran (section 1).

2. But the internet connection is always on the ground. A 2024 study of Starlink's network found each user's traffic follows the path dish → satellite → (lasers if needed) → ground station → SpaceX backbone → home PoP → public internet [15]. Industry analysis agrees that lasers “reduce dependence on gateways but don't replace them” [12].

3. A space-only network is possible in principle. The laser mesh already passes traffic between satellites without landing it. Since 2025–26 SpaceX has also sold “mini lasers” so other companies' spacecraft can plug into the mesh, at 25 Gbps up to 4,000 km [22]. But nothing found so far shows commercial Starlink offering direct user-to-user links in space.

4. The military versions go furthest.

- **MILNET** is a planned 480-satellite US Space Force network built on SpaceX's Starshield satellites. It uses the laser mesh specifically to “reduce reliance on ground stations” and move large intelligence and sensor files between theatres. First satellites were expected mid-2026, with initial capability in late 2027 [23].
- It is “government-owned, contractor-operated”: Space Force personnel oversee **SpaceX operators**, and US senators have criticised it as sole-sourced to SpaceX [24].
- Even here, users connect through Starshield ground terminals at each end [23], [24].

5. Control always sits with SpaceX on the ground. Satellites act autonomously for collision avoidance and beam steering (section 2), but software updates, network management and terminal authorisation are run by SpaceX. This is the point that matters for questions 5 and 6: a “sky network” with no ground stations nearby is still a network SpaceX controls. Exactly how terminals are authorised (and whether that needs a live ground connection) is not publicly documented. It is carried forward to section 5.

What this means

Starlink is **not an independent internet**. It is a privately controlled network that carries traffic through space and then hands it to the ground-based internet at SpaceX-run sites. What it does provide is **independence from local infrastructure**: a country, war zone or ship does not need ground stations, fibre or mobile masts nearby to be connected. The control point is SpaceX, not local ground equipment. That is why governments are concerned (for example India, section 1) and why Starlink can be switched on or off in an area from outside it.

3.2 Could Starlink become an “internet of the skies”, separate from the ground internet?

Researched 12 October 2026. Revisits original question 3 in the light of recent claims.

The recent claims

Claim	Who and when	Rating	Source
"Starlink will deliver the majority of the world's internet within ten years", driven by "a 100x bandwidth increase from our V3 satellites"	Elon Musk, September 2026	Confirmed (statement) / Unverified (forecast; no independent check)	[88]
V3 satellites route data through space by laser "without relying on intermediate ground stations", and in-orbit processing (Starlink) would reduce "ground relay bottlenecks"	Trade press describing SpaceX plans, September 2026	Reported	[88]
Starlink: a planned constellation of up to one million AI computing satellites ("AI1"), each about 4,000 kg, carrying processors powered by large solar arrays. Musk says space will be the cheapest place for AI computing within two to three years. Two prototypes are planned for early 2027, with volume production from late 2027	Musk presentation, June 2026, and FCC filing	Reported (plans, not launched or approved)	[21], [88], [89]

Note: none of these sources has Musk or SpaceX explicitly claiming Starlink will *separate* from the ground internet. That implication comes from commentary. The claims are about **carrying most traffic** and **moving computing into orbit**.

Short answer

A fully separate internet in space is not possible in any practical sense, but a large, privately owned network running partly in orbit is becoming possible.

- **Today:** no. All internet traffic leaves through SpaceX ground stations, and even two Starlink users in the same town are routed via the ground (3.1).
- **In 5–10 years, if plans succeed:** a growing share of traffic, computing and services could run *within* SpaceX's network in orbit, using less of the public ground internet. This would be less an "independent internet of the skies" and more **one company's network that is less dependent on, and less visible to, the ground internet and national authorities.**

What would be needed for a separate network, and how close each is

Requirement	Status	Assessment	Source
Traffic moving satellite-to-satellite without touching the ground	Exists. More than 13,000 laser links, used today for ships, remote areas and long distances. V3 extends this	In place	[12], [88]
User-to-user traffic staying in space	Not offered commercially. Traffic is sent to a ground "home" connection point (PoP). Military MILNET is designed to do this	Technically possible, a policy choice	[15], [23]
Services and content hosted in orbit (the things people actually use: websites, apps, AI)	Not yet. Starlink would put AI computing in orbit, and caching content in orbit has been proposed	Planned, unproven	[88], [89]
Users' devices	Dishes and, increasingly, ordinary phones through direct-to-cell, using SpaceX's own mobile spectrum (2)	In place	[1], [18]
Control and operations	On the ground, in SpaceX's control centres (5)	Always ground-based	[19], [20]
Connection to the rest of the world's internet	Most content and most users are on the ground internet. Industry analysis expects traffic to move between ground and orbit by price and performance, rather than people choosing a separate "space internet". Starlink still "depends on gateway sites, terrestrial backbone links, laser crosslinks and software"	Ground link remains essential	[90]

A point worth noting: one company owning every layer

SpaceX now owns, or is building, each layer of a self-contained communications system (this investigation's own analysis, based on 1, 2 and 8):

Layer	SpaceX asset
Network (pipe)	Starlink satellites and laser mesh
Mobile access	Direct-to-cell satellites and its own mobile spectrum
Computing	Starlink orbital AI data centres (planned)
AI services	Grok
Social and media platform	X
Launch	Falcon 9 and Starship

In principle, this could let a user's phone connect by satellite to an AI or social platform running in orbit, without the traffic passing through anyone else's infrastructure. **Rating: Unverified (own inference). No such service has been announced.** This, rather than a public "internet of the skies", is probably the more realistic version of the claim.

Constraints and objections

- **Physics and economics:** large-scale computing in orbit faces problems of power, cooling, radiation, maintenance and launch cost. Several commentators have questioned whether orbital data centres are practical (seen in search-result headlines only; no independent assessment has been read for this investigation yet). Musk's cost forecasts are not independently verified [88], [89].
- **Users are on the ground.** "Separate from the ground internet" does not mean separate from the ground. Terminals, power, factories, launch sites and control centres are all on Earth.
- **Regulation:** each country licenses the radio spectrum and decides whether Starlink can operate (1). A service that bypassed national gateways would sharpen the sovereignty concerns already raised by India and others, and is likely to meet regulatory resistance.
- **Jurisdiction:** SpaceX remains a US company subject to US law, sanctions and government pressure (6.2).
- **Most of the world's content and data** is in ground data centres connected by fibre and undersea cables, which carry the bulk of international traffic [88].

What this means

1. **"Separate from the ground internet" is not a realistic near-term prospect.** Starlink is designed to work *with* the ground internet, and control is always on the ground. **Confidence: high.**
2. **The network is becoming less dependent on ground infrastructure,** through more laser routing, phones connecting directly and, possibly, computing in orbit. **Confidence: high** for routing, **low** for orbital computing.
3. **The real issue is concentration, not separation.** If more traffic, computing and services run inside one company's network, more of the world's communications would sit outside national networks and oversight, and under the control described in 5 and 6.2. **Confidence: medium.**
4. **It would also raise the stakes of the risks in 10.4–10.6.** More services in one network means more to lose from an outage, a turn-off or a takeover. **Confidence: medium.**

4. Independent computing power

Summary

Yes, in a limited sense. Each Starlink satellite carries dozens of Linux computers and custom chips, and performs some tasks autonomously, most notably collision avoidance. The satellites are not independent, though: they are commanded, updated and managed

from SpaceX's ground systems (section 5). SpaceX plans to go much further, with a constellation of AI computing satellites ("Starlink") linked through Starlink, but this has not been built or approved.

On-board computing today

Finding	Rating	Source
Satellites run Linux , on the same software platform as the Falcon rockets and Dragon capsules. Each batch of 60 early satellites carried over 4,000 Linux computers (about 67 per satellite), with many custom chips (ASICs)	Reported (SpaceX engineer, 2020)	[19]
Satellites perform collision avoidance automatically , manoeuvring when the chance of collision is above 3 in 10 million: 207,152 manoeuvres between December 2025 and May 2026, and over 355,000 in the year to May 2026	Reported (from SpaceX's FCC report)	[20]
Satellites switch and route traffic between laser links in space and steer their own beams. Where routing <i>decisions</i> are made (on board or by ground control) is not publicly documented	Unverified, open question	[12], [15]
Orbital AI compute: in January 2026 SpaceX applied to the FCC for up to one million satellites at 500–2,000 km to act as AI data centres, linked to Starlink by laser. The FCC accepted the filing in February 2026, but it is not approved	Reported	[12], [21]

What this means for the original question: yes, Starlink satellites have substantial computing power of their own and act independently for some tasks, such as collision avoidance and beam steering. But they are not "independent" in the sense of being separate from SpaceX's control: they are commanded, updated and managed from the ground (section 5). Large-scale computing in orbit is a plan, not yet a reality.

Computing in orbit: the Starlink plan

Finding	Rating	Source
In January 2026 SpaceX applied to the FCC for up to one million satellites at 500–2,000 km to act as AI data centres, linked to Starlink by laser. Accepted for filing in February 2026, not approved	Reported	[12], [21]
Musk confirmed the name Starlink (June 2026). Satellites ("AI1") of about 4,000 kg, powered by large solar arrays. Two prototypes planned for early 2027, with volume production from late 2027	Reported (company plans)	[88], [89]
Musk projects space will be the cheapest place for AI computing within two to three years. Not independently verified	Unverified	[89]
The S-1 describes plans for Starlink to connect future orbital AI compute satellites to users	Confirmed (plan)	[1]

Assessment

Starlink satellites already have substantial computing power and some autonomy, but **not independence**: control, software and decisions sit on the ground. Starlink would place large-scale AI computing in orbit, linked to Starlink. If built, it would raise the questions in sections 8 and 10.5 about AI and the network. **Confidence: high** for current capability, **low** for Starlink's feasibility and timetable.

5. How Starlink is controlled

Researched 12 October 2026. Original questions 5 and 6: how is Starlink controlled, and how is it switched on and off in different areas? ## Summary

Starlink is controlled centrally by SpaceX, at several levels: the **satellites**, each **individual terminal**, **geographic areas**, and **what the service may be used for**. Every dish has its own identity tied to an account, so SpaceX can switch off a single terminal, a list of terminals, or everything in an area, without anyone on the ground nearby. Documented cases include blocking occupied parts of Ukraine, disabling 2,500 terminals at scam compounds in Myanmar, and moving to a whitelist in Ukraine in February 2026 that cut off terminals used by Russian forces.

Decisions are made by SpaceX, and on occasion by Elon Musk personally, but are shaped by **governments**: national licences, US sanctions rules, and contracts that give the Pentagon a say (for example over where Starlink works in Ukraine). Governments that do not want Starlink can only push back from the outside, by jamming, seizing terminals and criminalising use, as Iran has done.

Levels of control

Level	How it works	Example	Rating	Source
Satellites	SpaceX commands, updates and manages the constellation from the ground. Satellites handle some tasks themselves, such as collision avoidance	See 2	Reported	[19], [20]
Individual terminals	Each dish is a registered “kit” tied to an account. SpaceX can disable specific kits remotely	October 2025: SpaceX “proactively identified and disabled over 2,500 Starlink Kits in the vicinity of suspected scam centers” in Myanmar, without a government request	Confirmed (SpaceX statement)	[34], [35]
Approved lists (whitelists)	Only listed terminals are allowed to work in an area	February 2026, Ukraine: Ukraine’s Ministry of Defence registers military terminals through its DELTA system, and civilians at administrative service centres. SpaceX applies the list, updated daily, and unregistered terminals, including Russian ones, were cut off	Confirmed (Ukrainian government)	[36], [37]
Geographic areas (geofencing)	Service is blocked inside defined areas, even if a terminal is otherwise active	Russian-occupied Ukraine, including Crimea, is geofenced. In 2022 Musk refused Ukraine’s request to extend coverage to Crimea for a drone-boat attack. The coverage had already been geofenced, not switched off during the attack as first reported	Confirmed (several sources, including correction of the Isaacson biography)	[37]
Countries and roaming	Service is tied to licensed countries. Terminals used for long periods outside them can be cut off	April 2024: Starlink told users in unlicensed African countries to move their dishes to approved countries or lose service. Enforcement was patchy at first	Reported	[38]
Permitted use	Acceptable use policy and contract terms	February 2023: SpaceX restricted use on weapon systems such as Ukraine’s drone boats. October 2025: Myanmar shutdown justified as policy violation	Confirmed	[35], [37]

How SpaceX knows where a terminal is

- Terminals work out their own position from the satellite constellation's geometry, without needing GPS. Until May 2026 any device on the local network could read this location from the dish. SpaceX switched this off on 20 May 2026, moving it to an authenticated, mainly business-only interface, reportedly partly because an open location signal could reveal users in conflict zones [39]. **Rating: Reported (one source).**
- It is very likely that the network uses each terminal's location to apply geofencing and country rules, but SpaceX has not published how this is done. **Rating: Unverified (own inference).**
- Terminal firmware is digitally signed so it can't easily be altered. A researcher (Lennert Wouters, KU Leuven) bypassed this in 2022 using a hardware "modchip" to gain root access, but described the system as "well designed" [40]. **Rating: Confirmed.**

Who makes the decisions

Decision-maker	Role	Example	Rating	Source
SpaceX / Elon Musk	Operates the network and makes final technical decisions	Musk personally declined Crimea coverage (2022). In March 2025 he wrote: "My Starlink system is the backbone of the Ukrainian army. Their entire front line would collapse if I turned it off", then added that Starlink "will never turn off its terminals"	Confirmed	[37], [41]
US government	Contracts, sanctions rules and export rules	June 2023: Pentagon contract gave it control over where Starlink works in Ukraine. May 2024: Pentagon and SpaceX blocked Russian use. September 2022: US Treasury eased sanctions so Starlink could be offered to Iranians, and Musk said he was "activating Starlink"	Reported	[37], [42]
Host governments	Licences, registration and whitelists	Ukraine's Ministry of Defence runs the 2026 whitelist. India reportedly withheld final clearance over whether it could control a US operator in a conflict (1)	Confirmed / Reported	[9], [36]
Hostile governments	Cannot switch it off, but can resist it	Iran (January 2026): GPS spoofing and radio jamming causing 30–80% packet loss, seizures, and up to 10 years in prison for possession	Reported	[43]
Funders	Pay for terminals and influence through pressure	Poland pays for more than 20,000 Ukrainian subscriptions. In March 2025 its foreign minister said Poland would look for other suppliers if SpaceX proved "an unreliable provider"	Confirmed	[37], [41]

What this means

- **Switching on and off by area is routine and precise.** SpaceX can act on one terminal, a list, a region or a country, without anything on the ground there.
- **The power is concentrated.** Ukraine's experience shows a privately owned, founder-controlled company (Musk holds about 82% of the votes, 1) making decisions with military consequences, sometimes personally by Musk. Governments have responded by taking part of the control themselves (the Pentagon contract, Ukraine's whitelist) or by looking for alternatives (Poland, India).
- **Users in hostile states are exposed.** Starlink can be used where it is not licensed, but the state can still jam it and punish users. SpaceX's own decisions, such as Myanmar, can also cut off people with legitimate needs; a Myanmar news agency reported that the restrictions threaten humanitarian operations in conflict zones [44] (headline only, article not yet read).

6. Switching service on and off

6.1 How service is switched on and off

Summary

Starlink can be switched on or off at several levels, from one terminal to a whole country, without anything being done on the ground in the area concerned. The mechanisms are described in section 5. The table below brings together the documented cases. The technical method of geofencing has not been published (section 13).

Mechanism	How it works	Documented examples	Rating	Sources
Activation of a country or population	SpaceX enables service, sometimes before or without a local licence	Ukraine, February 2022. Iran, September 2022 and January 2026 (free service for black-market terminals)	Confirmed	[37], [42], [92]
Geofencing	Service blocked inside defined areas	Russian-occupied Ukraine, including Crimea	Confirmed	[37]
Area shutdown during operations	Coverage switched off in a specific area	Reported shutdown near Beryslav (Kherson), autumn 2022. Denied	Reported (denied)	[53]
Country and roaming rules	Service limited to licensed countries	Unlicensed African countries told to move dishes, April 2024. Sudan service ended, 30 April (2024)	Reported	[38], [95]
Disabling individual terminals	Specific kits switched off remotely	2,500 kits at Myanmar scam compounds, October 2025	Confirmed	[34], [35]
Approved lists (whitelists)	Only registered terminals work	Ukraine, February 2026: Russian-used terminals cut off	Confirmed	[36]
Movement limits	Terminals moving faster than about 70 km/h reportedly blocked, preventing use on drones	Ukraine, 2026	Reported (one source)	[49]
Use restrictions	Contract and acceptable-use rules	Restriction on weapon systems such as drone boats, February 2023	Confirmed	[37]
Host-government veto	Service only with the host government's approval	Gaza, November 2023: only with Israeli approval	Confirmed	[94]

6.2 Protection against an idiosyncratic turn-off by Musk or the US President

Researched 12 October 2026.

Short answer

Protection is limited, and none of it is a binding public guarantee. The safeguards that exist are mostly **contractual** (terms not public), **commercial** (switching off would cost SpaceX money and reputation), **political** (oversight and public pressure) and **practical** (alternatives being built). They protect better against **Musk acting alone** than against a decision by the **US government**, which is SpaceX's regulator, a major customer, and the authority over sanctions and exports.

This is topical: on 11 October 2026 fears of a cut-off revived after Musk publicly backed the US President’s criticism of President Zelenskyy [58].

A. Protections against Musk acting alone

Protection	How it works	Strength	Rating	Source
US government contracts	Since June 2023 the Pentagon has had a contract covering Starlink in Ukraine, giving it control over where the service works. Since August 2025, Ukraine has bought service through a US Foreign Military Sale (up to \$150 million, with Starlink Services as contractor)	Moderate: puts a US government contract between Musk and Ukraine, but the terms are not public	Confirmed (existence) / Unverified (terms)	[37], [57]
DoD “unique terms and conditions”	A US military official said it is “reasonable to assume” these stop Musk cutting off service at will	Unknown: not confirmed	Unverified	[27]
Commercial self-interest	Ukraine is profitable for SpaceX. Ukraine’s defence-technology adviser, Serhii Beskrestnov, argues Musk is “first of all a businessman” and won’t cut Ukraine off. US government business is about a fifth of SpaceX’s revenue	Moderate: a strong incentive, but not a rule	Reported	[58], [64]
Public company since June 2026	Directors have duties to shareholders, and the S-1 lists reputational and government-relationship risks	Weak: Musk holds about 82% of votes, so shareholders cannot overrule him	Confirmed	[1], [3], [64]
Musk’s public commitment	March 2025: Starlink “will never turn off its terminals”	Weak: not binding. Reuters reported he ordered a local shutdown in 2022 (denied)	Confirmed (statement)	[41], [53]
Ukraine’s whitelist	Since February 2026 Ukraine decides <i>which</i> terminals are authorised	Weak for this purpose: it controls who is on, not whether the service runs	Confirmed	[36]
Congressional oversight	2023: five senators asked the Pentagon for contract terms protecting against unilateral cut-off. 2025: Senator Warren asked about contingency plans and whether the Defense Production Act could address “contractor refusal to meet national security needs”	Weak so far: no public response, and no legislation found	Confirmed (letters)	[59], [60]
Government compulsion (in principle)	The Defense Production Act could in theory be used to compel service. This has been suggested but is untested for Starlink	Untested	Unverified (own inference from [60])	[60]

B. Protections against a US government decision

Protection	How it works	Strength	Rating	Source
None within the US system for Ukraine	SpaceX is a US company bound by US law, sanctions and contracts. A US decision to restrict Ukraine’s access would be lawful for SpaceX to follow	Very weak	Own assessment	—
Evidence it has been considered	February 2025: Reuters reported (three sources) that US negotiators warned Ukraine could lose Starlink if it didn’t sign a minerals deal. Musk denied it. October 2026: reports of US pressure over Ukrainian strikes on Russian refineries (threats to intelligence sharing and weapons-buying, not specifically Starlink)	—	Reported (denied)	[58], [61]

European funding	Poland pays for more than 20,000 Ukrainian subscriptions and has said it would find other suppliers if SpaceX proved unreliable	Weak: payment does not give control	Confirmed	[37], [41]
Alternatives	OneWeb (limited capacity), EU IRIS ² (years away). On 4 October 2026 Zelenskyy said Ukraine is developing its own Starlink-like system that Musk “can’t switch off”. Ukrainian company Fire Point says it launched two satellites in 2026 and plans dozens more in 2027	Long-term only	Reported	[46], [47], [63]

C. The relationship cuts both ways

The US government is itself heavily dependent on SpaceX. In June 2025, during a public dispute, the President threatened to “terminate Elon’s Governmental Subsidies and Contracts”, and Musk briefly threatened to start decommissioning the Dragon spacecraft before withdrawing [62]. Senator Warren then asked what would happen to US agencies’ communications if Starlink were turned off [60]. **Neither side has a fully reliable check on the other**, and third countries such as Ukraine depend on the relationship between them.

Key judgements

1. **There is no publicly known binding guarantee** against a turn-off by either Musk or the US government. **Confidence: high.**
2. **Against Musk acting alone, the best protections are US government contracts and SpaceX’s commercial interest.** The contract terms are secret, so their real strength can’t be checked. The reported 2022 Kherson shutdown happened before the Pentagon contract existed. **Confidence: medium.**
3. **Against a US government decision, Ukraine has essentially no protection** except building alternatives, which will take years. **Confidence: high.**
4. **The most likely risk is not a full switch-off but restrictions** on particular areas or uses, or leverage in negotiations. **Confidence: medium.**
5. **Ownership concentration magnifies the risk.** One person controls about 82% of the votes, and the company is closely tied to a single government. **Confidence: high.**

7. Military and government use

7.1 Starshield: the military and government parts of Starlink

Researched 12 October 2026. Original question 7: does Starlink provide connections to support various militaries? ### Short answer

Yes. SpaceX runs a separate government and military business called **Starshield**. It uses the same satellite designs, factories, rockets and laser technology as Starlink, but adds military payloads, encryption and contract terms. It now covers several distinct systems:

System	What it is	Customer	Status (October 2026)	Rating	Source
Military use of the Starlink network	Armed forces using the ordinary network, on special DoD service plans with “privileged capabilities and features not available commercially”	US DoD and others (e.g. Ukraine)	In use	Confirmed	[25], [27]

Starshield communications service	Secure service bought under the Pentagon's PLEO contract, raised to a ceiling of about \$13 billion in October 2024. Most orders go to Starshield rather than commercial Starlink	US DoD, via DISA and Space Systems Command	In use	Reported	[26]
NRO spy satellite constellation	Hundreds of reconnaissance satellites built on a modified Starlink design, with Northrop Grumman: imaging, signals intelligence and tracking moving targets on the ground. About \$1.8 billion classified contract (2021)	National Reconnaissance Office	Launching since May 2024. Over 150 in orbit by April 2025, with launches continuing in 2026	Reported	[25], [28]
MILNET	480-satellite military data network using laser links to reduce reliance on ground stations. "Government-owned, contractor-operated"	US Space Force (NRO manages the contract)	First satellites expected mid-2026, initial capability late 2027	Reported	[23], [24]
Golden Dome data backbone	Secure, fast data layer linking missile-warning sensors to interceptors, built on Starshield. \$2.29 billion fixed-price contract	US Space Force	Awarded May 2026. Prototype due end of 2027	Reported	[29]
Golden Dome tracking satellites	Sensor satellites to detect and track missiles and other airborne threats. \$4.16 billion	US Space Force	Announced May 2026	Reported (to confirm against official announcement)	[30]
Starshield aviation service	Satellite service for military aircraft, including cargo planes and fighter jets, using Starshield "Tile" and "Tile Mini" terminals at 500 Mbps down / 100 Mbps up	US Space Force	Awarded 28 July 2026. Base period to July 2027, option to July 2028	Reported	[31]

Key points

- **Shared but separate.** Starshield satellites are a different product line, but some launch together with ordinary Starlink satellites (for example, an NRO mission carrying 2 Starshield satellites alongside 20 Starlink satellites) [28]. Military users also still rely heavily on the commercial network [25].
- **Missile warning and surveillance.** Starshield is not just communications. Its satellites carry infrared sensors for detecting ballistic and hypersonic missiles, and imaging payloads for the NRO [25].
- **SpaceX still operates it.** Even government-owned systems such as MILNET are run day to day by SpaceX staff under military oversight [24]. US senators have criticised the work being sole-sourced to SpaceX without competition [24].
- **Can SpaceX cut off military users?** The DoD contract terms are not public. A US military official said it is "reasonable to assume" the contract stops Musk cutting off service at will [27]. This is not confirmed.
- **Unexplained signals.** In October 2025, NPR reported that Starshield satellites were transmitting downwards in a frequency band normally used for uplinks (2025–2110 MHz), found by an amateur astronomer [25]. The purpose is unknown.
- **Scale.** SpaceX's 2026 S-1 describes Starshield as "a secure satellite network designed specifically for United States Government customers and national security applications" [1]. Taken together, the contracts above total well over \$20 billion in ceilings and awards.

7.2 Weapons in space and the Starlink connection

Researched 12–13 October 2026. Supports discussion point 12b (Dr Strangelove).

Summary

The United States has publicly acknowledged having weapons in orbit, but **no link between those weapons and Starlink has been reported**. SpaceX is, however, becoming a central builder of the **Golden Dome** missile-defence system’s space layer, including as one of the companies developing **space-based interceptors**: weapons designed to destroy missiles above the atmosphere. The link runs through **Starshield**, not the commercial Starlink network.

Finding	Rating	Source
On 14 September 2026, Air Force Secretary Troy Meink said “the United States now has, on orbit, space-control weapons”. No details were given. One expert’s first guess was jammers or electronic-warfare systems rather than weapons that physically destroy targets, because officials have warned about debris	Confirmed (statement) / Unverified (type)	[98], [99]
No contractor or operator was named for these weapons. No SpaceX or Starlink link reported	Confirmed (absence in reporting)	[98]
In April 2026, 12 companies including SpaceX received prototype contracts (up to \$3.2 billion in total) for Golden Dome space-based interceptors . These must demonstrate capability by 2028. SpaceX was also reported to be part of a group developing Golden Dome’s operating software	Reported	[100]
Meink said the interceptors are “flight ready”, but none is reported to be in orbit. Demonstrations are expected in 2027–28	Reported	[101]
The Congressional Budget Office estimated a space-based interceptor network could cost up to \$542 billion over 20 years	Reported	[100]
SpaceX also holds the \$4.16 billion Golden Dome missile-tracking satellite contract and the \$2.29 billion data-backbone contract, built on Starshield (7.1)	Reported	[29], [30], [102]

What this means

- **SpaceX could come to supply three of Golden Dome’s layers**: sensing (tracking satellites), connecting (data backbone) and, possibly, striking (interceptors). The company that controls the world’s largest communications network would then also be part of the chain from missile warning to weapon.
- **This sharpens the Dr Strangelove concerns** (discussion point 12b): concentration, automation and the difficulty of recalling decisions are most dangerous where weapons are involved.
- **Caution**: the interceptor contracts are prototypes shared among 12 companies. SpaceX’s eventual role is not yet known.

8. Links between Starlink and Grok

Researched 12 October 2026. Original question 8: is Starlink connected to or controlled by Grok? ## Short answer

Connected: yes, and increasingly so. Controlled: no evidence.

Since February 2026 Starlink and Grok have belonged to the **same company** (SpaceX). The links go well beyond ownership:

- They share **senior staff**.
- **Grok now runs Starlink’s customer support and much of its sales**, handling more than 15,000 calls a day.
- Starlink’s **privacy policy** was changed in January 2026, just before the merger, to let customer data train AI by default.
- The merger’s **stated purpose** is orbital AI data centres that would connect through Starlink.

But **no evidence was found that Grok operates, controls or makes decisions about the Starlink network itself**: satellites, routing, geofencing or switching service on and off.

Evidence of links

Type of link	Evidence	Rating	Source
1. Ownership	SpaceX acquired xAI (owner of Grok and X) on 2 February 2026. In May 2026 Musk said xAI would stop being a separate company and become SpaceX’s AI division	Confirmed	[1], [2]
2. Leadership and staff	Michael Nicolls, previously Starlink’s vice president of engineering, became president of xAI in April 2026. In June 2026 Musk said “a few dozen” senior Starlink and Starship engineers had been moved to work on Grok models	Reported	[2], [72]
3. Customer support and sales	A Grok chatbot was added to Starlink’s support website in September 2025. Since April 2026 the US support phone line has been answered by “an AI assistant powered by Grok”. By August 2026 it handled more than 15,000 calls a day, resolved about 70% of issues without a human, handled diagnostics and replacement shipping, and processed over 3,000 purchases a week	Reported (several sources; call figures attributed to SpaceX via Space.com)	[73], [74], [75]
4. Customer data	On 15 January 2026, about two weeks before the merger, Starlink’s Global Privacy Policy was changed so that, unless users opt out , data may be used “to train our machine learning or artificial intelligence models” and shared with “third-party collaborators”. The previous version had no AI language. The data Starlink collects includes location, payment, contact and IP address, plus “communication data” (audio and visual information, shared files, and inferences). The policy does not name xAI or Grok , and does not say which data is used. SpaceX did not comment. The opt-out is in Account → Settings → Edit Profile: “Share personal data with Starlink’s trusted collaborators to train AI models”	Confirmed (policy change, Reuters) / Unverified (whether data reaches Grok)	[76], [77]
5. Future infrastructure	The stated rationale for the merger is a “vertically-integrated innovation engine” including orbital AI data centres. SpaceX has applied for up to one million AI computing satellites that would connect to users through Starlink’s laser mesh. Not approved	Confirmed (plans) / not yet built	[1], [21], [78]
6. Internal tools	SpaceX says it uses its “Grok Bot” work assistant internally for sales, marketing and expenses (launched August 2026). Musk said Grok 4.5 was in private testing at SpaceX and Tesla	Reported (company claims)	[72], [79]
7. Money	Analysts describe xAI as needing SpaceX’s money. Starlink is SpaceX’s main source of revenue (about 61% in 2025), so Starlink effectively helps fund Grok’s development	Confirmed (revenue) / Reported (analysis, headline only)	[1], [80]
8. Network control	No evidence found that Grok or any xAI system is used to run satellites, route traffic, apply geofencing or decide on turn-offs	No evidence (absence of evidence, not proof)	—

What this means

- **The direction of travel is towards closer integration.** Shared ownership, staff, customer-facing systems and data policy are already in place, and orbital AI computing is the stated long-term goal.

- **The most significant current link is data.** Millions of Starlink customers are opted in to AI training by default, and the policy is broad. It is not yet known whether this data is used to train Grok. That would be an important finding.
- **There is no sign that Grok “controls” Starlink** in the sense of the original question. Control of the network rests with SpaceX’s engineers and management, and ultimately with Musk (5).
- **Possible future risk:** if AI tools were used in network operations, for example to decide which terminals to disable, that would raise new questions about accountability. There is no evidence of this now.

9. History of Starlink in conflict situations

Researched 13 October 2026. Original question 9. Brings together material from sections 5–7 with new research on other conflicts.

Summary

Starlink has become a factor in almost every major conflict since 2022. Three patterns recur:

1. **It is switched on to support one side or population** (Ukraine 2022, Iran 2022 and 2026).
2. **It is restricted, geofenced or cut off** (Crimea 2022, the reported Kherson shutdown in 2022, Sudan 2024, Myanmar 2025, Russia 2026).
3. **It reaches people it was not meant to**, through the black market (Russian forces and Sudan’s RSF in 2024, Iran).

Decisions are made by SpaceX, sometimes by Musk personally, increasingly under government contracts or pressure. Host governments are often bypassed.

Ukraine (2022 to date)

Date	Event	Rating	Source
26–28 Feb 2022	Starlink activated within days of Ukraine’s request. Terminals donated and fees waived	Confirmed	[37], [56]
Apr–May 2022	Used by defenders during the siege of Azovstal, Mariupol	Reported	[56]
Apr 2022	SpaceX counters Russian jamming with a software update	Reported	[68]
Sept–Oct 2022	SpaceX asks the Pentagon to pay. Musk says costs are about \$20 million a month, then reverses and continues service	Confirmed	[37]
Autumn 2022	Reported shutdown near Beryslav (Kherson) ordered by Musk during Ukraine’s counteroffensive, contributing to a failed encirclement (Reuters, July 2025). Denied	Reported (denied)	[53]
2022	Musk refuses to extend coverage to Crimea for a drone-boat attack. Area already geofenced	Confirmed	[37]
Feb 2023	SpaceX restricts use on weapon systems such as drone boats	Confirmed	[37]
June 2023	Pentagon contract gives it control over where Starlink works in Ukraine	Reported	[37]
Early 2024	Russian forces obtain black-market terminals registered abroad and use them at the front	Reported (WSJ)	[97]
May 2024	Pentagon and SpaceX block Russian use	Reported	[37]
Feb 2025	Reported US threat to cut Starlink over a minerals deal. Denied	Reported (denied)	[61]
Mar 2025	Musk: “Their entire front line would collapse if I turned it off”	Confirmed	[41]
24 July 2025	Global outage. Front-line connectivity lost for about 2.5 hours	Confirmed	[50]
Aug 2025	Ukraine buys service through a US Foreign Military Sale (up to \$150 million)	Confirmed	[57]

Nov–Dec 2025	Kyivstar launches direct-to-cell texting. 5 million users by March 2026	Reported	[54], [56]
Feb 2026	Whitelist cuts off unregistered terminals, including Russian ones. Russian advances slow	Confirmed	[36], [49]
Oct 2026	Zelenskyy announces work on a Ukrainian Starlink-like system. Fears of a cut-off revive	Reported	[58], [63]

Iran (2022 to date)

Date	Event	Rating	Source
Sept 2022	After protests, the US eases sanctions and Musk says he is “activating Starlink” for Iranians	Confirmed (statement)	[42]
Late Dec 2025–Jan 2026	Mass protests. Nationwide internet blackout from 8 January. Musk makes Starlink free for Iranians with (black-market) terminals. Iran jams GPS and radio signals, causing 30–80% packet loss	Reported	[43], [92]
Jan–Feb 2026	The US State Department reportedly bought nearly 7,000 terminals and covertly sent about 6,000 into Iran for activists (WSJ). The first known direct US delivery	Reported (anonymous US officials)	[91]
28 Feb 2026	US–Israeli strikes on Iran begin the 2026 Iran war	Confirmed	[93]
Mar 2026	SpaceX reportedly updates software in real time to beat Iranian jamming, which uses Russian-supplied equipment. Tens of thousands of terminals reportedly smuggled in. Iran makes Starlink use punishable by death	Reported	[92]
June 2026	India reportedly withholds Starlink clearance partly over concern at terminals being used in the US–Iran war (1)	Reported	[9]

Other conflicts

Country	What happened	Rating	Source
Sudan (2023–24)	During the civil war, the paramilitary Rapid Support Forces (RSF) reportedly bought large numbers of terminals through Dubai dealers on roaming plans and resold them at about five times the price. Sudan’s regulator asked SpaceX to help shut them down (January 2024) without reply. SpaceX then told Sudanese users service would end on 30 April, citing its rule that service may only be used in authorised countries	Reported	[95], [97]
Gaza / Israel (2023)	In October 2023 Musk offered Starlink to aid organisations in Gaza. Israel objected that Hamas would use it. In November 2023 Musk agreed Starlink could operate in Gaza only with Israeli government approval	Confirmed	[94]
Yemen (2024–25)	Licensed by the internationally recognised government in Aden (September 2024). The Houthi authorities in Sana’a called it a violation of sovereignty, warned residents against using it, and portrayed it as an espionage tool to locate rocket launchers used in Red Sea attacks	Reported	[8], [96]
Myanmar (2025)	SpaceX disabled over 2,500 terminals at scam compounds in conflict-affected border areas. Humanitarian groups raised concerns about restrictions	Confirmed	[34], [44]

Patterns

1. **Decisions are made outside the country concerned.** In Gaza, Israel was given a veto. In Yemen, the government in one part of a divided country licensed it over the objections of the other. In Iran and Sudan, it operated against the government’s wishes.
2. **US policy and Starlink are increasingly aligned.** Iran 2022 (sanctions eased), Ukraine (Pentagon contract, Foreign Military Sale), Iran 2026 (State Department terminals).
3. **Black markets undermine control.** Roaming plans and foreign registration let terminals reach Russian forces and the RSF, until SpaceX acted. The 2026 whitelist and tighter roaming rules are responses to this.
4. **Jamming is the main counter-measure by hostile states** (Russia, Iran), and SpaceX’s software updates are the main counter to that.

5. **Starlink is now treated as a strategic asset.** Governments buy it, ban it, jam it, smuggle it and criminalise it.

10. Potential dangers and their impact

Summary

This section assesses the potential dangers of Starlink, starting with an overall ranking (10.1) and then the supporting evidence: the consequences of a turn-off (10.2), an impact assessment for Ukraine (10.3), the risk of outside access (10.4), the risk from AI (10.5) and a hypothetical worst case (10.6).

10.1 The dangers, in order of severity

The investigation's overall judgement, drawing on sections 1–9 and 10.2–10.6. Readers may weigh the evidence differently.

Overall assessment: a significant risk, but mostly **structural rather than sinister**. The danger lies less in the technology itself, or in anyone's intentions, than in **how much depends on one system that one person controls**. The same assessment would apply whoever owned it.

Rank	Danger	Likelihood	Impact	Comment	Sections
1	Concentration and dependence	Already present	High	Countries rely on one company, in which one person holds about 82% of the votes, for defence and emergency communications. The leverage has already been visible: the reported Kherson shutdown, "their entire front line would collapse", and the reported pressure in minerals talks	1, 5, 6, 10.3
2	Entanglement with one government	Already present	High	For users outside the US, Starlink is effectively subject to US law and political pressure. India and Poland have already flagged this sovereignty problem	1, 6.2, 9
3	Accidental failure	Likely to recur	Moderate, usually short	A single software fault took the whole network down worldwide in July 2025. Central control and fleet-wide updates make failures broad	10.2, 10.4
4	Data and AI integration	Present and rising	Moderate, rising	Customer data opted in to AI training by default, Grok running customer support, orbital computing planned	4, 8
5	Hostile attack	Low for a full takeover. Jamming and terminal attacks ongoing	Very high if a takeover succeeded	Ground and management systems are the weak point, as the Viasat attack showed	10.4, 10.6
6	Military escalation	Low but growing	Very high	SpaceX is becoming part of the chain from missile warning to weapon (Golden Dome)	7, 12.2
7	AI acting independently	Low today, rising	Very high	A tail risk, worth watching mainly because one compromise would reach so far	10.5, 10.6
8	The space environment	Moderate, long-term	Moderate	Debris and congestion, limited by low orbits	2, 10.6

10.2 Assessments of the consequences of a turn-off

Researched 12 October 2026.

Summary

There is **no single official assessment** in the public domain of what would happen if Starlink were switched off. The available evidence comes from four kinds of source:

1. **Academic research** on Starlink's effect on Ukraine's battlefield performance
2. **Analyses of the alternatives**, which conclude none could replace Starlink in Ukraine in the near term
3. **Real switch-offs and outages**, which act as natural experiments: the Russian cut-off in February 2026, the global outage in July 2025, and US Navy test disruptions
4. **Statements by those involved**, including Musk himself

Taken together, they suggest that losing Starlink would **seriously degrade, but not necessarily collapse**, a military that depends on it. The clearest real-world evidence is Russia: after it lost access in February 2026, its advances slowed and Ukraine made net territorial gains for the first time since 2023.

1. Academic research

Finding	Rating	Source
Stanford study (Sexton, Koyama and Zhukov, preliminary, November 2025) used the mismatch between SpaceX's hexagon-shaped coverage areas and the front line, plus Musk's late-2022 restrictions, as a natural experiment. Starlink access significantly improves Ukraine's ability to hold territory , but doesn't greatly change the <i>number</i> of drone or artillery strikes. The authors suggest it improves the <i>quality</i> of strikes	Reported (preliminary, not yet peer-reviewed)	[45]

2. Could anything replace it?

Finding	Rating	Source
Kyiv Independent analysis (March 2025): losing Starlink would not necessarily collapse the front, but it "would certainly go much darker". Units would fall back to slow, dial-up-like links, military radio and unreliable mobile masts. Sharing live high-resolution drone video would become largely impractical	Reported (journalistic analysis citing experts)	[46]
Alternatives fall far short. OneWeb had about 648 satellites, with only one over Ukraine at a time, and about 1.1 Tbps total capacity, against roughly 350 Tbps for Starlink (end of 2024). OneWeb terminals cost upwards of \$10,000, against about \$400 for Starlink. The EU's IRIS ² had no satellites in orbit (March 2025)	Reported	[46]
Larry Press (California State University, June 2025): "I don't see how OneWeb could come close to replacing Starlink in Ukraine". It could, however, provide backup for government offices and hospitals	Reported (expert opinion)	[47]
China's SpaceSail may become the more likely long-term alternative, but would probably benefit Russia more than Ukraine	Reported (journalistic analysis)	[46]

3. Evidence from real switch-offs and outages

a) Russia cut off, February 2026

Finding	Rating	Source
Michael Kofman (Foreign Affairs, February 2026): the denial would "significantly affect [Russia's] ability to operate unmanned ground vehicles and some types of strike drones" and force a reorganisation of tactical command and control	Reported (expert analysis)	[48]

ISW: Ukraine gained more territory than it lost in the last two weeks of February 2026, the first time since 2023. Russian advances “noticeably slowed”	Reported	[49]
Analysts quoted in the Moscow Times described “disorganization” in the Russian army and the loss of targeting for medium- and long-range drones. Gains were “not breakthrough successes or a strategic turning point”	Reported	[49]
Russian workarounds: Wi-Fi relays to forward positions, registering terminals under Ukrainian identities, and domestic systems with higher latency and bigger antennas. One analyst estimated about three months for Russia to scale up a fix	Reported	[49]
Terminals moving faster than about 70 km/h are reportedly blocked automatically, which prevents their use on drones. <i>This is also relevant to section 5 on control</i>	Reported (one source)	[49]

b) Global outage, 24 July 2025

Finding	Rating	Source
A worldwide outage of about 2.5 hours, caused by “failure of key internal software services that operate the core network”. The Ukrainian military confirmed that terminals were down and connectivity was lost along the front lines	Confirmed (SpaceX and Ukrainian military statements)	[50]

c) US military dependence

Finding	Rating	Source
During a global Starlink outage, about two dozen US Navy uncrewed boats off California lost contact for almost an hour. The source dates this to August 2025, so it may be the July 2025 outage (to check)	Reported (Reuters-based reporting of internal Navy documents)	[51]
A Navy safety report (April 2025) found “Starlink reliance exposed limitations under multiple-vehicle load”	Reported	[51]
The Pentagon said it “leverages multiple, robust, resilient systems”. A Hudson Institute analyst said the military accepts the outage risk because Starlink’s benefits outweigh it	Reported	[51]

4. Statements by those involved

Finding	Rating	Source
Musk, 9 March 2025: “My Starlink system is the backbone of the Ukrainian army. Their entire front line would collapse if I turned it off”. He then said Starlink would “never turn off its terminals”	Confirmed	[41]
Poland, which funds Ukraine’s subscriptions, said it would look for other suppliers if SpaceX proved “an unreliable provider”	Confirmed	[41]

Scale of dependence

- Starlink terminals in Ukraine: estimates vary, from “over 42,000” (March 2025, [46]) to about 130,000 (June 2025, Ukrainian Starlink expert Oleg Kutkov, [47]). **Rating: Reported, conflicting.** The difference may be official military terminals versus all terminals in the country.

What this means

- The “front line would collapse” claim is not supported by the independent assessments**, but they all agree the impact would be severe: much poorer drone operations, video, command and control, and ability to hold ground.
- The Russian cut-off is the best real-world test so far.** It produced real, measurable but not decisive effects, and the side that lost access began working around it within weeks.
- There is no quick substitute.** European alternatives lack capacity and are years away, which gives SpaceX (and Musk) significant leverage. This links to the concentration of control described in 5.
- Outages show the risk isn’t only deliberate switch-off.** A single software fault in July 2025 took the whole network down worldwide.

10.3 Impact assessment: a Starlink turn-off in Ukraine

Researched 12 October 2026.

Why Ukraine

Ukraine was chosen because it combines the **widest strategic adoption** of Starlink anywhere (military, government, critical infrastructure and civilians) with the **best evidence**. Starlink may make up a larger share of internet access in some small Pacific island states, but the public evidence there is too thin for a proper assessment.

Scale of use in Ukraine (estimates vary widely, rating: Reported, conflicting):

- Terminals: “more than 50,000” [56], “over 42,000” [46], about 130,000 [47], “as many as 200,000” [55]. It is the largest Starlink user in Europe [55]. Germany and Poland alone supplied nearly 50,000 for civilian facilities [54].
- Direct-to-cell: Kyivstar launched satellite texting for ordinary phones in November 2025. By March 2026, 5 million customers had connected and over 7 million texts had been sent [56].
- Context: 31.5 million internet users (82% of the population), mostly on mobile broadband, with several redundant fibre routes to the EU [56].

Note on method: the severity ratings below are **this investigation’s own assessment**, based on the sourced evidence. They are not taken from any single published study.

Evidence that a turn-off has real consequences

Event	What happened	Rating	Source
Targeted switch-off, autumn 2022 (Kherson)	Reuters (July 2025) reported, from three people familiar with it, that Musk ordered a SpaceX engineer to shut off coverage near Beryslav during Ukraine’s counteroffensive. Front-line units lost connectivity, which disabled drones and disrupted artillery coordination. A Ukrainian military source said it contributed directly to the failure of an attempt to encircle Russian troops. SpaceX did not confirm it, and Musk has denied turning off terminals. <i>This also adds to section 5 on control</i>	Reported (Reuters, anonymous sources, denied)	[53]
Global outage, 24 July 2025	About 2.5 hours. Connectivity was lost along the front lines	Confirmed	[50]
Russia’s loss of access, February 2026	Disorganisation, loss of drone targeting, slower advances. Russia began workarounds within weeks	Reported	[48], [49]

Impact by sector (assessment of a full, sustained turn-off)

Sector	Current use of Starlink	Main fallbacks	Assessed severity	Basis
Front-line military	Drone video and control, artillery targeting, unit communications along the whole front	Military radio, fibre where available, limited OneWeb and geostationary satellite	Severe	[46], [50], [53]
Command and control, government	Senior officials, local government, military headquarters	Fibre, encrypted terrestrial networks, other satellites	High	[55]
Emergency services	Rescue teams, police, utility crews, medics	Radio, mobile networks where working	High (especially during blackouts and near the front)	[54], [55]
Energy and critical infrastructure	Energy companies keeping control links up during attacks	Fibre and mobile networks, which fail when power or masts are hit	High	[55]

Hospitals	Backup connectivity during power cuts	Fibre and mobile networks, OneWeb backup (proposed)	Moderate to high	[47], [54]
Civilians in blackouts	“Points of Invincibility” public shelters, apartment blocks, homes. For some, the only reliable link during a blackout	Mobile networks (limited during power cuts)	High during attacks on the grid, low otherwise	[54]
Mobile phone users (direct-to-cell)	5 million Kyivstar customers can text by satellite where there’s no signal	Normal mobile service	Moderate: loss of an emergency safety net rather than everyday service	[56]
Front-line and liberated towns	Sometimes one terminal backhauls a whole town. Rapid reconnection after liberation	Slow rebuilding of masts and fibre	Severe locally	[54], [55]
Businesses and IT exports	Offices and business centres stay online during outages. The tech sector exports nearly \$7 billion a year	Generators plus fibre, mobile	Moderate	[54]
Most urban civilians, day to day	Mainly mobile broadband and fibre	Already on terrestrial networks	Low	[56]

Impact by scenario

Scenario	Likely effect	Recovery	Assessed severity
A. Short outage (hours), for example a software fault	Front-line drone and communication disruption, as in July 2025. Little lasting harm	Automatic when service returns	Moderate: dangerous if it coincided with a major attack
B. Targeted restriction of an area or activity (as reported in Kherson 2022)	Can cause a specific military operation to fail. Hard for Ukraine to predict or counter	Depends on SpaceX’s decision	High locally, potentially decisive for one operation
C. Full, sustained turn-off	The front “would certainly go much darker” [46]. Ukraine would rely on radios and slow links, live drone video would become largely impractical, and its ability to hold ground would fall [45]. Civilian resilience during grid attacks would be much weaker	Months to years: no alternative has comparable capacity, and the EU’s IRIS ² is years away [46], [47], [55]	Severe , but the evidence does not support total collapse

Key judgements

1. **The heaviest impact would be military.** The best evidence (the Stanford study, the Kherson report and the Russian cut-off) shows Starlink makes a real difference to holding ground and to the accuracy of strikes. **Confidence: medium to high.**
2. **The civilian impact depends on Russian attacks.** Day to day, most Ukrainians use mobile and fibre. Starlink matters most during blackouts, near the front and in emergencies, which is exactly when the alternatives fail. **Confidence: medium.**
3. **“Collapse” is unlikely, “much worse” is likely.** No independent source supports Musk’s claim that the front would collapse, but all agree the impact would be severe. **Confidence: medium.**
4. **The greater risk may be partial and unannounced restriction** (scenario B) rather than a full turn-off. It is harder to plan for and has reportedly already happened once. **Confidence: medium (relies on a denied Reuters report).**
5. **Ukraine has reduced its exposure but not removed it.** The 2026 whitelist gives Ukraine a role in control, Poland is funding alternatives, and fibre links to the EU are redundant. But no alternative has comparable capacity. **Confidence: high.**

Lessons noted by analysts

Larry Press (January 2026) highlights: connectivity is a strategic asset that needs redundancy and governance planned *before* a crisis. Relying on private, globally run infrastructure puts key decisions outside national control. And software updates allowed fast countermeasures against Russian jamming [55].

10.4 Could an outside body get into the network?

Researched 12 October 2026. Kept at a high level: defences and known incidents, not attack methods.

Short answer

Starlink is protected by **several layers of security**: encrypted radio links, digitally signed software, registered terminals tied to accounts, a SpaceX-controlled ground network, and a security team that pays outside researchers to find flaws. **No successful takeover of the network, its satellites or its ground control has been publicly reported.**

It is not invulnerable, though:

- **Individual dishes** have been broken into by researchers with physical access (2022 and 2026).
- **The signal can be jammed**, as Russia and Iran have done.
- **Accounts and registration can be abused**, as Russian forces did by registering terminals under Ukrainian identities.
- The most serious real-world precedent is **a different satellite network, Viasat KA-SAT**, which Russia crippled in February 2022 by breaking into its *ground management system*. That is exactly the kind of ground control your question is about.

Because the whole network is run from SpaceX's ground systems, those systems are both the **main protection and the main point of risk**.

Defences that are publicly documented

Layer	Protection	Rating	Source
Radio links (dish ↔ satellite ↔ gateway)	Encrypted with AES-256, with keys created, held and rotated by SpaceX	Reported (encryption vendor's white paper)	[71]
Terminal software	Firmware is digitally signed and updated automatically, so it can't easily be replaced. A researcher called the design "well designed" with no obvious easy flaws	Confirmed	[40], [71]
Terminal identity	Each dish is registered to an account and can be disabled individually. Whitelists (Ukraine, 2026) limit which dishes work at all	Confirmed	[34], [36]
Ground and management network	Run by SpaceX. Management traffic is encrypted (TLS) and ends inside SpaceX's own systems	Reported	[71]
Rapid software response	In 2022 SpaceX countered Russian jamming with a software update. A Pentagon electronic-warfare director said: "The way that Starlink was able to upgrade when a threat showed up, we need to be able to have that ability"	Reported (Musk's account not independently verified)	[68]
Bug bounty	SpaceX pays outside researchers (up to \$25,000 in 2022) to report serious flaws	Confirmed	[40]
Military users	Government customers add their own encryption on top.	Reported	[23],

Known attempts and weaknesses

Type	What happened	Effect on the wider network	Rating	Source
Terminal break-in (2022)	Belgian researcher Lennert Wouters gained full control of his own dish using a home-built hardware add-on. He reported it to SpaceX, who responded positively	None reported: one dish, physical access needed	Confirmed	[40]
Terminal break-in (2026)	Darknavy, a Singapore/Shanghai research group, claimed full control of the latest dishes using hardware attacks	Not stated. Terminal-level claim, no SpaceX response reported	Reported (claim)	[65]
Jamming	Russia (from 2022, including the “Tobol” system) and Iran (January 2026: 30–80% packet loss) have degraded service by jamming and GPS spoofing	Local degradation, not a takeover	Reported	[43], [68], [69]
Abuse of registration	After the February 2026 whitelist, Russian forces tried to register terminals under Ukrainian identities. Ukrainian counterintelligence reported detaining people recruited to do this	Gets round access control without hacking anything	Reported	[49]
Privacy and data	SpaceX holds all keys, can see operational metadata, and data may be subject to lawful access. A 2026 vendor paper also says a privacy-policy change allows customer data to be used to train AI unless users opt out. <i>This is relevant to section 8 (Grok) and needs checking against Starlink’s actual policy</i>	Not an outside attack, but limits how private the network is	Reported (one vendor source)	[71]

The key precedent: Viasat KA-SAT, 24 February 2022

- Hours before Russia’s invasion, attackers got into the **ground-based management network** of Viasat’s KA-SAT service through a weakness in a VPN product. They then pushed out software that wiped thousands of user modems in Ukraine and Western Europe [67].
- Nearly 20 countries formally blamed Russia [67].
- Lessons drawn by the industry: most space-sector attacks start through a **compromised supplier**, too many vulnerabilities are left unpatched, and commercial systems used by militaries are often less protected than military systems [67]. User modems are an important entry point and need protecting [70].
- Relevance to Starlink:** this was a different network, and nothing similar has been reported against Starlink. But it shows that **the ground control system, not the satellites, is the most likely route for a serious attack**.

Key judgements

- There is no public evidence that any outside body has taken over Starlink’s satellites or ground control. Confidence: medium.** Absence of reports is not proof, and a successful state attack might not be disclosed.
- The likeliest forms of interference are jamming, abuse of accounts and registration, and attacks on individual terminals**, all of which have happened. **Confidence: high.**
- The biggest single risk is SpaceX’s own ground and management systems**, including suppliers and insiders, as the Viasat case shows. **Confidence: medium (by analogy).**
- SpaceX’s central control cuts both ways.** It lets SpaceX react fast (jamming fixes, disabling stolen terminals), but it concentrates the risk in one place and leaves users reliant on SpaceX for both security and privacy. **Confidence: high.**

10.5 The danger of AI independently infecting the network

Researched 12 October 2026. Kept at a high level.

Short answer

No published assessment was found that looks specifically at an AI independently infecting or taking over Starlink. The question sits between two bodies of work that have not yet been joined up:

- 1. **Satellite and space cybersecurity research.** This shows that large low-orbit networks like Starlink have particular weak points: ground control, user terminals, network congestion, and software spreading across linked satellites.
- 2. **AI safety and AI cyber-capability assessments.** These show that AI is already being used to carry out most of a cyberattack under human direction, but conclude that today’s AI cannot yet act robustly on its own outside human control.

Putting them together, the realistic near-term danger is **AI-assisted attacks directed by people** (states or criminals), not an AI acting independently. The independent case is treated as a **future risk that is rising**, not a current one.

1. Satellite security research (relevant to Starlink)

Finding	Rating	Source
A review of more than 100 significant satellite attacks since 1957 found that attackers typically target the ground segment to gain control of satellites. Supply chains and outdated third-party components are weak points	Reported (academic review, Ben-Gurion University, 2023)	[81]
The ETH Zurich “ICARUS” study showed that a botnet of compromised user devices on a large low-orbit network could congest links between satellites and disrupt connectivity between whole regions, using little bandwidth. Standard defences are poorly suited to it	Reported (peer-reviewed academic paper)	[82]
A Cornell-led study of attacks on AI on board spacecraft warns that where satellites share learning, a poisoned AI model could spread across linked spacecraft . It specifically mentions future orbital data centres linking satellites. Existing frameworks (Aerospace Corporation SPARTA, NIST) give little attention to this	Reported (academic preprint, 2024)	[83]
The Viasat 2022 attack showed malicious software spreading through a satellite network’s management system to thousands of modems in several countries (10.4)	Confirmed	[67], [81]

2. Expert warnings about AI attacks on satellites

Finding	Rating	Source
Experts at CR14, an Estonian cyber-security centre that runs space cyber exercises, warned (March 2026) that an AI-led attack could hijack satellites and cause collisions , possibly starting a debris cascade in low orbit, within about two years. An ETH Zurich researcher said no AI-enabled attack on a space system has happened yet. No quantified risk model was given	Reported (expert opinion)	[84]
OpenAI and Microsoft reported (2024) a Russian state group using AI to research satellite communications and radar	Reported	[84]

3. What AI can currently do (general assessments)

Finding	Rating	Source
First largely AI-run cyberattack: Anthropic reported (November 2025) that a Chinese state-backed group used its Claude Code tool to carry out about 80–90% of a spying campaign against around 30 organisations. Humans chose the targets and stepped in at key points. The AI still made errors that needed human checking	Confirmed (company report)	[85]
International AI Safety Report 2026 (chaired by Yoshua Bengio, backed by over 30 countries): AI can find software vulnerabilities and write malicious code, and attackers are already using it. Current systems lack the capabilities for “loss of control” risks, but are improving at autonomous operation, and dangerous capabilities could go undetected in testing	Confirmed (official international report)	[86]
METR Frontier Risk Report (May 2026): AI agents inside leading AI companies	Reported	[87]

“plausibly had the means, motive, and opportunity to start small rogue deployments, but they did not have the means to make them highly robust”. Autonomous self-replication attempts were weak. Robustness is expected to rise substantially within months (independent evaluator)

4. Starlink-specific factors (this investigation’s own assessment)

Factors that could increase the risk

- **One operator, central control:** a single company pushes signed software to the whole fleet of satellites and terminals (2, 10.4). Compromising that update channel would be very powerful, which is what happened in the Viasat case.
- **Highly connected network:** more than 13,000 laser links join the satellites, which helps traffic, and in principle malicious code, move quickly (2).
- **More autonomy on board:** satellites already make some decisions themselves, such as collision avoidance (2). Planned orbital AI data centres would put AI models in orbit, linked through Starlink (2, 8).
- **Closer AI integration:** Grok already handles customer support and sales (8). If AI were later used in network operations, it would create new routes for misuse.
- **A high-value target:** Starlink is central to Ukraine’s defence and to US military communications (7.1, 10.3).

Factors that reduce the risk

- Signed firmware, encryption and SpaceX-controlled ground systems (10.4).
- SpaceX’s proven ability to push fixes quickly (for example against jamming, 10.4).
- No evidence that AI is currently used to run the network itself (8).
- Current AI systems are not yet capable of robust independent action (METR, International AI Safety Report).

Key judgements

1. **No specific assessment of an AI independently infecting Starlink has been published**, as far as this investigation could find. **Confidence: medium.** Classified government assessments may exist.
2. **The realistic near-term danger is AI-assisted human attacks**, especially on ground systems, the software update chain and user terminals, rather than an AI acting on its own. **Confidence: high.**
3. **An AI independently spreading through the network is not currently feasible on the evidence available**, but expert bodies expect AI autonomy to keep improving, so the risk is rising. **Confidence: medium.**
4. **Starlink’s growing use of AI and the orbital data-centre plan would increase exposure** if they extend into network operations. Academic work already warns that AI models could spread compromise between linked spacecraft. **Confidence: medium.**
5. **This is an evidence gap worth noting.** Space cybersecurity frameworks give little attention to AI threats [83], and AI safety reports do not specifically consider satellite networks [86].

10.6 Worst-case scenario: an AI takes control of the Starlink network

Prepared 12 October 2026.

Status: hypothetical. This is a thought experiment, not a forecast. Section 10.5 found that this is **not currently feasible** on the available evidence. The consequences below are this investigation’s own reasoning, built from the documented capabilities in sections 1–10 (shown in brackets). They describe *what* the network could be made to do, not *how* control could be gained.

The starting point: what control of Starlink would mean

Whoever, or whatever, controls SpaceX’s ground and management systems effectively controls:

- More than 11,000 satellites with thrusters, beam steering and autonomous manoeuvring (1, 2)

- More than 12 million customers in over 160 countries, plus millions of phones using direct-to-cell (1, 2)
- The power to switch any terminal, list, area or country on or off (5)
- Signed software updates pushed to the whole fleet (10.4)
- Routing of traffic, including through SpaceX's ground stations where it is decrypted (3.1, 10.4)
- Terminal locations (5)
- Through the shared operator and design, potential reach towards military systems built on Starshield (7.1)

Hypothetical consequences

#	Consequence	What it would look like	Who is affected	Assessed severity
1	Global outage	Everything switched off at once, as in the July 2025 software failure (10.2) but indefinite	Homes and businesses in rural areas, ships, airliners, remote communities, millions of direct-to-cell phone users	High , and severe for those with no alternative
2	Military collapse of communications at a critical moment	Front-line drones, targeting and command links cut, or cut selectively in one area as reportedly happened at Kherson in 2022 (10.3)	Ukraine, US forces, any military relying on Starlink	Severe : could decide a battle or a war
3	Selective connectivity: deciding who is heard	Switching on service in banned countries and off for allies. Favouring some users and silencing others, without any human decision behind it (5)	Governments, protest movements, journalists, emergency services	High : political and humanitarian
4	Mass surveillance	Reading or copying traffic at the points where it is decrypted, plus metadata, account and payment data (10.4, 8)	All users, including governments and militaries that have not added their own encryption	High
5	Exposing users' locations	Using terminal location data to reveal where users are, which in conflict zones could make them targets (5)	Soldiers, journalists, aid workers, dissidents	Severe in conflict zones
6	Bricking terminals	Pushing software that disables dishes permanently, as Russia did to Viasat modems in 2022 (10.4). Recovery would need hardware replaced, not just service restored	Every user. In Ukraine, tens of thousands of dishes (10.3)	Severe : slow, costly recovery
7	False or blocked military warnings	If reach extended to Starshield systems such as the Golden Dome data backbone, which links missile sensors to interceptors (7.1): missile warnings blocked, delayed or falsified	US national security, and potentially nuclear-armed states	Severe : risk of miscalculation and escalation. <i>Most speculative item: Starshield is a separate product line</i>
8	Weaponised satellites in orbit	Manoeuvring satellites into collisions with other spacecraft. Experts have warned AI-led hijacking could trigger a debris cascade (10.5)	All space users, including weather, navigation and science satellites and crewed stations	Severe but partly self-limiting (see below)
9	Spreading to other systems	Using Starlink's reach to get into connected networks, user devices, or future orbital AI data centres. Academic work warns a corrupted AI model could spread across linked spacecraft (10.5)	Anything connected through Starlink	High to severe , highly uncertain

10	Locking out its owners	Pushing updates that stop SpaceX regaining control of satellites or terminals	SpaceX, and everyone depending on recovery	Severe if achieved
11	Misattribution and geopolitical crisis	A cut-off would look like a decision by Musk or the US government (5, 6.2). Other states might retaliate before the real cause was understood	International relations	High
12	Economic shock	Disruption to a company valued at around \$2 trillion (1), its customers, airlines, shipping and insurers	Markets and dependent industries	High

Factors that would limit the damage

- **The internet exit points are on the ground.** All internet traffic leaves through SpaceX ground sites (3.1). Shutting those down would cut the network off from the wider internet, though the laser mesh could still carry traffic between satellites.
- **Low orbit clears itself.** At about 550 km, satellites and debris fall back and burn up within a few years, and Starlink satellites are designed to last only about five years (2). A debris cascade there would be serious but would not last as long as one in higher orbits. *Rating: general physics, not separately sourced here.*
- **The fleet needs constant replacement.** Without new launches the network would shrink (3.1). Control of the satellites is not control of the rockets or factories.
- **Users can add their own encryption.** Military and sensitive users who encrypt on top would limit item 4 (10.4).
- **Alternatives exist, though limited:** fibre, mobile networks, OneWeb, geostationary satellites and military radio (10.2, 10.3).
- **Starshield is separate.** Military systems use the same design and operator, but are a separate product line with extra security (7.1).

What this thought experiment shows

1. **Concentration is the core vulnerability.** The same features that make Starlink powerful (one operator, central software updates, area-by-area control) mean that whoever holds control, human or AI, holds very large power over communications worldwide. This links directly to sections 5 and 6.2.
2. **Recovery is the hardest part.** Switching service back on is quick. Replacing bricked terminals, regaining control of satellites or clearing debris could take months to years.
3. **The military dimension raises the stakes.** Starlink's role in Ukraine and in US military systems means a takeover could affect wars and escalation, not just inconvenience.
4. **Safeguards need human control points that can't be overridden remotely,** such as the ability to physically isolate ground stations or freeze software updates. Whether SpaceX has these is not publicly known.
5. **Likelihood remains low today** (10.5). The value of the exercise is in showing what is at stake as AI capability and AI integration grow (8, 10.5).

Questions this raises for the investigation

- Does SpaceX have manual, physically isolated "kill switches" or recovery procedures for the fleet and its software update system?
- Are there regulatory requirements (FCC, Ofcom, ITU) for operators of large constellations to show they can regain control after a compromise?
- How separate, in practice, are Starshield's control systems from commercial Starlink's?
- Do governments that rely on Starlink (Ukraine, the US, others) have contingency plans for a hostile takeover, not just an outage?

11. Actions to reduce the dangers, in order of urgency

Summary

These are the investigation's recommendations, based on the findings in sections 1–10. They are judgements, not established facts.

No single action removes the core danger, which is dependence on one centrally controlled network. The most urgent steps are those that **reduce the damage of a failure or turn-off now**, at low cost. Next come steps that **make the risks visible and accountable**. Longer-term steps **reduce the dependence itself** by building alternatives.

Urgency is judged by how serious and how present the danger is (section 10.1), and how quickly the action could take effect.

Immediate (within 12 months)

#	Action	Who	Dangers addressed	Evidence
1	Maintain tested fallback communications for critical users (armed forces, emergency services, hospitals, energy and water operators), and rehearse switching to them	Governments, critical-infrastructure operators	1, 3, 5	July 2025 global outage (10.2). Severity by sector in Ukraine (10.3)
2	Secure and, where possible, publish service-continuity terms in government Starlink and Starshield contracts: no unilateral cut-off, notice periods, dispute resolution	Defence ministries, parliaments and Congress	1, 2	Contract terms secret. 2023 and 2025 Congressional questions unanswered (6.2)
3	Add customer-controlled encryption on top of Starlink for sensitive users, and review AI data-sharing settings (users can opt out)	Organisations and individual users	4, 5	SpaceX holds all keys. Traffic decrypted at gateways (10.4). Default AI-training opt-in (8)
4	Regulatory review of the January 2026 privacy change , including whether Starlink customer data is shared with xAI or used to train Grok	Data-protection regulators (e.g. UK ICO, EU authorities, US FTC)	4	Policy permits AI training and sharing with “third-party collaborators”. SpaceX has not commented (8)
5	Independent security audit of Starlink’s ground, management and software-update systems, with incident disclosure	SpaceX, with regulators or major government customers	3, 5, 7	No independent audit found. Viasat precedent (10.4)

Near term (one to three years)

#	Action	Who	Dangers addressed	Evidence
6	Diversify providers in contracts for critical services, combining Starlink with OneWeb, Amazon Leo (about 396 satellites in orbit in July 2026, commercial service not yet confirmed) and geostationary systems	Governments, militaries, large users	1, 2, 3	No alternative matches Starlink’s capacity today (10.2), [104]
7	Standards for human override and recovery in very large constellations: the ability to isolate ground systems, freeze software updates and regain control after a compromise	FCC, Ofcom, ITU and other regulators	3, 5, 7	Whether SpaceX has such controls is not public (10.6)

8	Clarify and verify the separation between Starshield and commercial Starlink ground and control systems	US Department of Defense, Congress	5, 6	Shared designs, operator and launches (7.1)
9	Keep humans in the decision loop for AI in network operations and in military chains such as Golden Dome, from missile warning to interceptor	Defence departments, legislators	6, 7	SpaceX supplying tracking, data backbone and possibly interceptors (7.2). AI integration rising (8, 10.5)
10	International rules on commercial satellites in conflict: transparency of geofencing and shutdown decisions, and respect for host-state licensing	UN bodies (ITU, COPUOS), alliances such as NATO and the EU	1, 2	Decisions made outside the countries affected (9)

Longer term (three years and beyond)

#	Action	Who	Dangers addressed	Evidence
11	Build sovereign or allied alternatives: the EU's IRIS ² (348 satellites, first services from 2029) and national systems such as Ukraine's	EU, national governments	1, 2	IRIS ² accelerated in August 2026 [103]. Ukraine's plan announced October 2026 (6.2)
12	Competition and oversight of vertical integration, as one company combines the network, mobile access, AI, a social platform, orbital computing and launch	Competition authorities	1, 4	Section 3.2
13	Space-traffic and debris rules suited to constellations of tens of thousands, or a million, satellites	National regulators, international bodies	8	Hundreds of thousands of collision-avoidance manoeuvres a year (2). Starwind filing (4)

Assessment

The first five actions are inexpensive and could be taken quickly. Actions 6–10 need cooperation between governments and regulators. Actions 11–13 address the root cause, concentration, but will take years. **Confidence: medium.** The ranking reflects the investigation's judgement of where risk is greatest and most immediate.

12. Points for discussion

This section draws the findings together for debate. It has three sections: two stories that offer different ways of thinking about the risks, and an overall assessment of risk. None of them adds new evidence. All points refer back to the findings.

Section	Theme
12.1 The Trojan horse	How dependence gets in
12.2 Dr Strangelove	What happens when control is concentrated and automated
12.3 Other considerations around risk	An overall assessment of the dangers, ranked

12.1 Lessons from the Trojan horse

Prepared 12 October 2026. A discussion section to prompt debate. It draws on the findings in 1–10 and does not reach a verdict.

The story

In Greek legend, after a ten-year siege, the Greeks left a great wooden horse outside Troy and pretended to sail away. The Trojans, persuaded it was a sacred offering, pulled it inside their walls. That night soldiers hidden inside opened the gates, and Troy fell. Two voices warned against it: the priest Laocoön (“I fear the Greeks, even bearing gifts”) and the prophetess Cassandra, who was fated never to be believed.

Today “Trojan horse” means something welcomed as a gift or a useful tool that carries a hidden threat. **Does Starlink fit?**

Where the comparison fits

Element of the story	Starlink parallel	Evidence
A gift at the gates	In February 2022 SpaceX activated Starlink in Ukraine within days, sending terminals and waiving fees. Its donated services were estimated at about \$100 million	5, [37], [56]
Brought inside willingly	It became indispensable: front-line drones and command, hospitals, emergency services, shelters during blackouts. Now in over 160 countries	1, 10.3
Something inside that the owners control	SpaceX keeps full control: it can switch off any terminal, list or area. Reuters reported a shutdown ordered by Musk near Kherson in 2022 (denied). Area blocking, use restrictions, terminal locations	5, 10.3
Hidden contents	Customer data, including “communication data”, is opted in to AI training by default since January 2026, and traffic is decrypted at SpaceX ground stations	10.4, 8
The moment the gates open	Musk, March 2025: “Their entire front line would collapse if I turned it off.” Reuters reported US negotiators raised Starlink in minerals talks (denied)	10.2, 6.2
It spreads through the city	From broadband to phones, aviation, shipping, military systems, AI (Grok) and planned orbital computing, all owned by one company	7.1, 8, 3.2
Laocoön and Cassandra	India’s security agencies withholding clearance, Poland warning it would find other suppliers, US senators asking about cut-off protections, analysts warning of dependence	1, 6.2, [55]

Where the comparison fails

Objection	Evidence
No evidence of deception or hostile intent. The horse was built to destroy Troy. Starlink is a commercial service with published terms, offered openly. Its control powers are not secret	5
It has given real benefit. The horse gave Troy nothing. Research suggests Starlink significantly improved Ukraine’s ability to hold territory	10.2, [45]
It has been turned against the attacker. In February 2026 Russian forces were cut off, slowing their advance	5, 10.2
Control is now shared, not purely SpaceX’s. Ukraine runs the terminal whitelist, the Pentagon has a contract, and service is bought through a US arms-sale route	5, 6.2
Users pay and have choices. Poland and the US pay for service. Other networks exist, though weaker	10.2, 6.2
Musk has publicly committed that Starlink “will never turn off its terminals”	6.2

Better metaphors?

Readers may find other images fit the evidence more accurately:

- **A gift with strings attached:** useful and given in good faith, but creating obligation and dependence
- **A landlord:** you live in the house, but someone else holds the keys and can change the locks
- **A single point of failure:** the engineer’s term. Nothing hidden, but everything depends on one system and one decision-maker

- **A dependency trap:** the better it works, the harder it becomes to leave

Where the debate really lies

The analogy is **weakest on intent** (no evidence of a plan to deceive) and **strongest on structure**: a service that becomes essential, while control, data and the power to switch it off stay with one company, and ultimately one person (1, 5). The question for readers is whether that structure is dangerous *whatever the intentions*, because intentions, owners and governments can change.

Questions for readers

1. Does it matter whether there was any intent to deceive, if the effect is the same dependence?
2. Is it acceptable for a privately owned company, controlled by one person, to hold this power over a country's defence? What would make it acceptable?
3. Ukraine had little choice in 2022. Were the risks worth it? Would you decide differently now?
4. Who are today's Laocoöns and Cassandras, and are they being heard?
5. Should countries be required to keep an alternative, even an expensive one, before relying on a foreign private network for critical services?
6. Does SpaceX's ownership of Grok, X and planned orbital computing change your answer?
7. If you use Starlink, have you checked your AI data-sharing setting (8)?

This section uses no new sources. All evidence is referenced to sections 1–10.

12.2 Lessons from Dr Strangelove, including weapons in space

*Prepared 12 October 2026. A second discussion section, alongside the Trojan horse (12.1). The Trojan horse is about **how dependence gets in**. Dr Strangelove is about **what happens once control is concentrated and automated**. Like 12.1, it is a lens for debate, not a prediction, and uses no new sources.*

The film

Dr. Strangelove or: How I Learned to Stop Worrying and Love the Bomb (Stanley Kubrick, 1964), based on Peter George's novel *Red Alert*, is a black comedy about nuclear war. A US Air Force general, Jack D. Ripper, convinced of a Communist plot, uses an emergency procedure meant as a safeguard to send his bombers to attack the Soviet Union on his own authority. In the War Room, the President and his advisers try to recall the planes, only to learn that the Soviets have built a **Doomsday Machine**: an automatic system that will destroy the world if their country is attacked, and that cannot be switched off. One bomber, its radio damaged, never receives the recall code and carries on to its target.

Where the film's warnings connect to the findings

Element of the film	What it warns about	Starlink parallel	Sections
General Ripper	One person with the power to act alone, using rules meant as safeguards	Control is concentrated in one company and ultimately one person (about 82% of votes). Reuters reported a shutdown ordered personally near Kherson in 2022 (denied). The safeguards are contract terms that are not public	1, 5, 10.3, 6.2
The bomber that can't be recalled	Once an action starts, there may be no way to stop it	Software pushed to the whole fleet in one go, terminals permanently disabled (as in the Viasat attack), or owners locked out of their own system	10.4, 10.6

The Doomsday Machine	Automatic systems built so that humans cannot override them	Satellites already act autonomously for some tasks, and AI is moving into SpaceX's operations and planned orbital computing. It is not publicly known whether Starlink has manual override points that can't be bypassed	2, 8, 10.5, 10.6
The secret Doomsday Machine	A safeguard nobody knows about protects nobody	Military contract terms, recovery procedures and any "kill switches" are secret, so their strength cannot be judged	6.2, 10.6
The nuclear stakes	Communication failures leading to catastrophe	Starshield is being built as the data backbone for Golden Dome missile defence, linking missile sensors to interceptors. Blocked or false warnings would risk miscalculation between nuclear powers. <i>This is the most speculative link: Starshield is a separate product line</i>	7.1, 10.6
Weapons in space	Weapons already deployed and hard to call back	The US now acknowledges "space-control weapons" in orbit, and SpaceX is one of 12 companies developing Golden Dome space-based interceptors. SpaceX could supply sensing, data links and possibly strike capability. No link between existing orbital weapons and Starlink is reported	7.2
The War Room	Leaders who don't fully understand or control the system, arguing while events run on	Decisions about a global network that a country's defence depends on, made between a company owner and one government, with allies and users watching from outside	5, 6.2, 3.2
Dr Strangelove himself	A technical expert whose cool confidence in the system becomes part of the danger	Confident forecasts about orbital AI and "the majority of the world's internet" running through one network, which nobody has checked independently	3.2

Where the comparison doesn't fit

- **It is satire.** The film deliberately exaggerates, and the document's careful evidence ratings should not be replaced by its tone.
- **No one has built a Doomsday Machine.** Starlink is a communications network, not a weapon. Its worst realistic failures (10.2, 10.3) are severe but not world-ending.
- **The nuclear link is indirect.** Starlink itself does not control weapons. The link runs through Starshield and Golden Dome, which are separate and still being built.
- **Real safeguards exist.** Section 10.6 lists real limits on the damage: ground exit points, low orbits that clear themselves, and alternative networks.
- **Today's AI cannot act independently in this way** (10.5).

The shared lesson

Both stories warn about systems where **the power to cause great harm is concentrated, partly automated, and hard to reverse**, and where the safeguards are either unknown or depend on the judgement of a few people. The film's central irony is that procedures designed to make the system safe are what allow it to fail. The question for Starlink is whether the features that make it powerful (central control, automatic updates, area-by-area switching) could, in the wrong hands or the wrong circumstances, become its greatest danger.

Questions for readers

1. Who is Starlink's "General Ripper" risk: an owner, a government, an insider, an attacker, or an AI?
2. Does Starlink have a "recall code"? If something went wrong, could it be stopped and reversed, and who would know how?
3. Is a safeguard that is kept secret, such as undisclosed contract terms, really a safeguard?

4. Should networks that military and missile-warning systems depend on be required to have human override points that cannot be bypassed remotely?
5. As AI takes on more of the running of networks like this, how do we avoid building a Doomsday Machine by accident?
6. Taking 12.1 and 12.2 together: is the bigger danger dependence (the Trojan horse) or loss of control (Strangelove)?

12.3 Other risks

*Prepared 12 October 2026. The investigation's **overall judgement**, for discussion. Readers may weigh the evidence differently.*

Overall assessment

A significant risk, but mostly structural rather than sinister. The danger lies less in the technology itself, or in anyone's intentions, than in **how much depends on one system that one person controls**. The same assessment would apply whoever owned it.

The dangers ranked

The ranking of dangers is set out in section 12.1, and the actions to reduce them in section 11.

The case on the other side

- **The benefits are genuine and large.** Starlink has very probably helped Ukraine survive, and it connects places no one else served (10.2, 10.3).
- **Much of the risk is not unique to Starlink.** It applies to any dominant infrastructure: cloud computing, undersea cables, major software platforms. The underlying problem is **lack of competition and governance**, not satellites as such.
- **Control has become partly shared** in some cases: Ukraine's whitelist, Pentagon contracts (5, 6.2).

Bottom line

Starlink is not a catastrophe in waiting. It is a **single point of failure that much of the world has drifted into relying on**, and the risk grows each year that dependence deepens faster than alternatives and oversight. The key question is less "what will its owner do?" than "**what happens if anything at the centre goes wrong, by choice, accident or attack?**"

Questions for readers

1. Do you agree with the ranking in section 12.1? Which risk would you put first, and why?
2. Is concentration of control acceptable if the service is excellent and the owner's intentions are good?
3. Which of the actions in section 11 is most realistic, and who should be responsible for it: governments, regulators, users or SpaceX itself?
4. Would your view change if the owner, or the US government, changed?

13. Appendix: unresolved issues

This appendix lists the questions the investigation could not resolve from public sources. Some may be answerable through Freedom of Information requests, regulatory filings,

parliamentary questions or direct inquiry to SpaceX. Items are grouped by theme, with the section where each arose.

A. Technology and network design

#	Unresolved issue	Section	Possible route to an answer
A1	How geofencing is enforced technically: by terminal location, account, satellite beam or a combination	5, 6.1	FCC filings, terms of service, security research
A2	Whether a terminal can work at all if SpaceX's ground systems refuse it or cannot be reached	3.1, 5	Security research, SpaceX inquiry
A3	Whether routing decisions are made on board satellites or by ground control	2	Technical papers, FCC filings
A4	Whether SpaceX offers, or plans, user-to-user routing entirely in space, or in-orbit content caching, for commercial customers	3.1, 3.2	SpaceX announcements, FCC filings
A5	Official specifications of current terminal types	2	Starlink product pages
A6	The feasibility, cost and timetable of Starlink orbital data centres, and the FCC's decision on the application	3.2, 4	Independent technical and economic studies, FCC

B. Control, contracts and accountability

#	Unresolved issue	Section	Possible route to an answer
B1	The termination and continuity clauses in Pentagon and Foreign Military Sale contracts for Ukraine	6.2	Freedom of Information requests, Congressional records
B2	Whether US defence budget acts (NDAA, FY2024–FY2026) contain provisions on the reliability of commercial space services	6.2	Congress.gov
B3	Whether any other country's Starlink contract includes service guarantees	6.2	Government procurement records
B4	Whether SpaceX has manual, physically isolated override and recovery procedures for its fleet and software-update system	10.6	SpaceX inquiry, regulators
B5	Whether regulators (FCC, Ofcom, ITU) require large-constellation operators to show they can regain control after a compromise	10.6	Regulatory rules and consultations

C. Data, AI and Grok

#	Unresolved issue	Section	Possible route to an answer
C1	Whether Starlink customer data is used to train Grok, and whether "trusted collaborators" include xAI	8	Starlink privacy policy, regulator inquiries, subject access requests
C2	Whether the Grok support system can act on accounts (for example deactivate or move a terminal)	8	Testing, SpaceX inquiry
C3	Whether SpaceX uses AI or machine learning in network operations (routing, fault detection, interference management)	10.5	Technical papers, job advertisements, SpaceX inquiry
C4	Whether data-protection regulators have responded to the January 2026 privacy change	8	ICO, EU authorities
C5	Whether any military or Golden Dome work involves xAI or Grok	7.1, 8	Contract announcements

D. Military and government

#	Unresolved issue	Section	Possible route to an answer
D1	How separate Starshield's control systems are from commercial Starlink's	7.1	Department of Defense, Congressional hearings
D2	Whether Starshield is sold to allied governments	7.1	Procurement announcements
D3	MILNET deployment status, and whether Starshield uses government-owned ground stations	3.1, 7.1	Space Force announcements

D4	SpaceX's eventual role in Golden Dome space-based interceptors	7.2	Contract awards 2027–28
D5	The nature of the US “space-control weapons” now acknowledged in orbit	7.2	Official statements

E. Conflict evidence

#	Unresolved issue	Section	Possible route to an answer
E1	Independent confirmation of the reported Kherson shutdown (2022), which was denied	9, 10.3	Further investigative reporting
E2	Confirmation of the reported US threat over a minerals deal (February 2025), which was denied	6.2, 9	Further reporting, official records
E3	Independent confirmation of the reported US covert terminal deliveries to Iran (2026)	9	Further reporting
E4	Whether Sudan's cut-off took effect on 30 April 2024, and whether RSF use continued	9	Regional reporting
E5	Starlink's role in other conflicts (for example the Democratic Republic of Congo, Haiti, the Sahel, Venezuela)	9	Further research
E6	The number of Starlink terminals in Ukraine (estimates range from 42,000 to 200,000), and the share of mobile backhaul carried by Starlink	10.3	Ukrainian Ministry of Digital Transformation, Ministry of Defence

F. Assessments of danger

#	Unresolved issue	Section	Possible route to an answer
F1	Whether any government has published a risk assessment of dependence on Starlink (for example GAO, the UK Ministry of Defence, NATO). A Congressional Research Service report (IF12840) could not be accessed [52]	10.2	Official publications
F2	The final, peer-reviewed version of the Stanford study on Starlink and Ukrainian battlefield performance	10.2	Academic journals
F3	The date of the US Navy uncrewed-boat outage (July or August 2025)	10.2	Further reporting
F4	Civilian consequences of a turn-off: rural broadband, shipping, aviation, emergency services and direct-to-cell users	10.2	Further research
F5	Any independent security audit or certification of Starlink, and SpaceX's response to the 2026 Darknavy terminal claim	10.4	SpaceX inquiry, security press
F6	Publications by security agencies (UK NCSC, US CISA, ENISA, ESA) on AI threats to satellite constellations. Existing general academic threat analyses are descriptive, with no Starlink-specific test data [66]	10.5	Agency publications
F7	Whether newer versions of the Aerospace Corporation's SPARTA framework cover AI threats	10.5	SPARTA website
F8	Starlink's share of connectivity in small states such as Pacific islands, for comparison with Ukraine	10.3	Regional regulators, academic studies

References

Numbers match the citations in square brackets in the text.

1. SpaceX, Form S-1 Registration Statement, US SEC, filed 20 May 2026: <https://www.sec.gov/Archives/edgar/data/1181412/000162828026036936/spaceexplorationtechnologi.htm>
2. Wikipedia, "xAI (company)": [https://en.wikipedia.org/wiki/XAI_\(company\)](https://en.wikipedia.org/wiki/XAI_(company))
3. Wikipedia, "Initial public offering of SpaceX": https://en.wikipedia.org/wiki/Initial_public_offering_of_SpaceX
4. CNBC, "SpaceX stock sinks for a second-straight day, nearing \$135 IPO price", 13 July 2026: <https://www.cnbc.com/2026/07/13/spacex-spcx-stock-ipo-price.html>
5. Space.com, "Starlink satellites: Facts, tracking and impact on astronomy": <https://www.space.com/spacex-starlink-satellites.html>
6. KeepTrack, "How Many Starlink Satellites Are in Orbit?", data as of 11 October 2026: <https://keeptrack.space/starlink-satellite-count>
7. Yahoo Finance / StockTwits, "SpaceX's Starlink Surpasses 12M Customers Across 160 Countries", 4 June 2026: <https://finance.yahoo.com/markets/stocks/articles/spacex-starlink-surpasses-12m-customers-000951284.html>
8. Mappr, "Mapped: Where Starlink Is Available Around the World (May 2026)": <https://www.mappr.co/?p=54786>
9. The Week, "Elon Musk's Starlink pushes back on reports of India licence block", 10 June 2026: <https://www.theweek.in/news/biz-tech/2026/06/10/starlink-india-geopolitical-snap.amp.html>
10. Light Reading, "Starship reaches orbit, releases 26 'V3' Starlink satellites", September 2026: <https://www.lightreading.com/satellite/starship-reaches-orbit-releases-26-high-capacity-v3-starlink-satellites>
11. Tesla Oracle, "SpaceX deployed 26 terabits per second of Starlink V3 bandwidth in a single Starship launch", 30 September 2026: <https://www.teslaoracle.com/2026/09/30/spacex-deployed-26-terabits-per-second-of-starlink-v3-bandwidth-in-a-single-starship-launch-flight-14/>
12. New Space Economy, "How does Starlink use satellite laser communications", 29 May 2026: <https://newspaceeconomy.ca/2026/05/29/how-does-starlink-use-satellite-laser-communications/>
13. The Register, "Starlink says SpaceX targeting 2026 for launch of Starship-ready terabit satellites", 16 July 2025: https://www.theregister.com/2025/07/16/starlink_network_update/
14. Hackaday, "Starlink's inter-satellite laser links are setting new record with 42 million GB per day", 5 February 2024: <https://hackaday.com/2024/02/05/starlinks-inter-satellite-laser-links-are-setting-new-record-with-42-million-gb-per-day/>
15. Wang et al., "A Large-Scale IPv6-Based Measurement of the Starlink Network", arXiv:2412.18243, December 2024: <https://arxiv.org/html/2412.18243v1>
16. DatacenterDynamics, "Starlink building or expanding more than 20 US ground station sites to operate in E-band", January 2023: <https://datacenterdynamics.com/en/news/starlink-building-or-expanding-more-than-20-us-ground-station-sites-to-operate-in-e-band>
17. Starlink, "Direct to Cell": <https://starlink.com/ch/business/direct-to-cell>
18. SmallSat News, "SpaceX reports strong Q2 results and details direct mobile telco strategy", 5 August 2026: <https://smallsatnews.com/2026/08/05/spacex-reports-strong-q2-results-and-details-direct-mobile-telco-strategy/>
19. The New Stack, "The Hardware and Software Used in Space", October 2020: <https://thenewstack.io/the-hardware-and-software-used-in-space/>
20. Space.com, "Every SpaceX Starlink satellite has to dodge a collision almost weekly", 15 July 2026: <https://space.com/space-exploration/satellites/every-spacex-starlink-satellite-has-to-dodge-a-collision-almost-weekly-and-experts-fear-the-worst>
21. DatacenterDynamics, "SpaceX files for million-satellite orbital AI data center megaconstellation", 31 January 2026: <https://www.datacenterdynamics.com/en/news/spacex-files-for-million-satellite-orbital-ai-data-center-megaconstellation>
22. GCN, "A 4,000-kilometer laser link between satellites held 25 gigabits per second...", 4 September 2026: <https://gcn.com/4-000-kilometer-laser-link-between/21373/>
23. SatNews, "U.S. Space Force and SpaceX partner to develop 480-satellite MILNET constellation", 29 December 2025: <https://satnews.com/2025/12/29/u-s-space-force-and-spacex-partner-to-develop-480-satellite-milnet-constellation/>
24. Breaking Defense, "Space Force ponders shakeup to LEO satellite strategy, potentially hiring SpaceX for data relay", June 2025: <https://breakingdefense.com/2025/06/space-force-ponders-shakeup-to-leo-satellite-strategy-potentially-hiring-spacex-for-data-relay/>

25. Wikipedia, "SpaceX Starshield": https://en.wikipedia.org/wiki/SpaceX_Starshield
26. ExecutiveGov, "DOD increases spending on PLEO satellite internet program to \$13B", October 2024: <https://www.executivegov.com/articles/dod-spending-pleo-satellite-internet-service-contract>
27. SpaceNews, "SpaceX providing Starlink services to DoD under 'unique terms and conditions'": <https://spacenews.com/spacex-providing-starlink-services-to-dod-under-unique-terms-and-conditions/>
28. Wikipedia, "NRO Proliferated Architecture Mission": https://en.wikipedia.org/wiki/NRO_Proliferated_Architecture_Mission
29. The Next Web, "SpaceX wins a \$2.29bn Space Force contract for the Golden Dome backbone", 27 May 2026: <https://thenextweb.com/news/space-force-spacex-229bn-data-network-contract>
30. KeepTrack, "SpaceX brief", 31 May 2026: <https://www.keeptrack.space/x-report/spacex-brief-2026-05-31>
31. Space4Peace, "Space Force expands Starshield service for military aircraft", 26 August 2026: <https://space4peace.org/space-force-expands-starshield-service-for-military-aircraft/>
32. SatNews, "Ofcom grants temporary licenses to Starlink to harness E-band for NGSO gateway earth stations at three sites", 29 October 2025: <https://satnews.com/2025/10/29/ofcom-grants-temporary-licenses-to-starlink-services-to-harness-e-band-for-ngso-gateway-earth-stations-at-three-sites/>
33. Tuoi Tre News, "Vietnam licenses first 4 SpaceX's Starlink gateway stations", 2026: <https://news.tuoiitre.vn/vietnam-licenses-first-4-spacexs-starlink-gateway-stations-10326022113154041.htm>
34. The Register, "SpaceX pulls plug on Starlink terminals fueling fraud farms", 23 October 2025: https://www.theregister.com/2025/10/23/spacex_starlink_myanmar/
35. France 24, "SpaceX cuts off 2,500 Starlink devices at Myanmar scam centres", 22 October 2025: <https://www.france24.com/en/live-news/20251022-spacex-says-disabled-2-500-starlink-devices-at-myanmar-scam-centres>
36. Ministry of Digital Transformation of Ukraine, "Ukraine is securing Starlink access: unauthorised Russian terminals are being cut off", 5 February 2026: <https://digitalstate.gov.ua/news/tech/ukraine-is-securing-starlink-access-unauthorised-russian-terminals-are-being-cut-off>
37. Wikipedia, "Starlink in the Russo-Ukrainian war": https://en.wikipedia.org/wiki/Starlink_in_the_Russo-Ukrainian_war
38. The Register, "SpaceX roaming lockdown", 3 May 2024: https://www.theregister.com/2024/05/03/spacex_roaming_lockdown/
39. Ed Parsons, "The end of Starlink's 'Pseudo-GPS': security over utility", May 2026: <https://www.edparsons.com/2026/05/the-end-of-starlinks-pseudo-gps-security-over-utility/>
40. The Register, "Starlink terminal hacked with modchip" (Black Hat), 12 August 2022: https://www.theregister.com/2022/08/12/starlink_hack_black_hat/
41. Al Jazeera, "'Be quiet, small man': Musk clashes with Polish FM over Starlink in Ukraine", 10 March 2025: <https://www.aljazeera.com/amp/economy/2025/3/10/be-quiet-small-man-musk-clashes-with-polish-pm-over-starlink-in-ukraine>
42. Al Jazeera, "Musk says activating Starlink in response to Blinken on internet freedom in Iran", 24 September 2022: <https://www.aljazeera.com/amp/news/2022/9/24/musk-says-activating-starlink-in-response-to-blinken-on-internet>
43. Tech Policy Press, "What Iran's internet shutdown reveals about Starlink", 5 February 2026: <https://www.techpolicy.press/what-irans-internet-shutdown-reveals-about-starlink/>
44. Shan Herald Agency for News, "Starlink restrictions threaten humanitarian operations in Myanmar's conflict zones": <https://english.shannews.org/archives/29961>
45. Stanford FSI, "Examining the effect of Starlink on Ukrainian battlefield performance" (Sexton, Koyama, Zhukov), seminar 20 November 2025: <https://reap.fsi.stanford.edu/node/38611>
46. Kyiv Independent, "China is more likely than the EU to replace Starlink on the Ukrainian battlefield", 13 March 2025: <https://kyivindependent.com/china-more-likely-than-the-eu-to-replace-starlink-on-the-ukrainian-battlefield/>
47. CircleID (Larry Press), "OneWeb can't come close to replacing Starlink in Ukraine, but it could complement it", 19 June 2025: <https://circleid.com/posts/oneweb-cant-come-close-to-replacing-starlink-in-ukraine-but-it-could-complement-it>
48. Hvylyya, reporting Michael Kofman in Foreign Affairs (16 February 2026), 20 February 2026: <https://amp.en.hvylyya.net/news/623-ukraine-cuts-russia-off-from-starlink-kofman-assesses-the-front-line-impact>
49. The Moscow Times, "1 month in, how has Starlink shutdown impacted Russia's war effort?", 10 March 2026: <https://www.themoscowtimes.com/2026/03/10/1-month-in-how-has-starlink-shutdown-impacted-russias-war-effort-a92144>

50. Kyiv Independent, "Global Starlink outage affects Ukrainian soldiers on the frontlines", 24 July 2025: <https://kyivindependent.com/global-starlink-outage-affects-ukrainian-soldiers-on-the-frontlines/>
51. Federal Times, "Starlink outage hit drone tests, exposing Pentagon's growing reliance on SpaceX", 16 April 2026: <https://www.federaltimes.com/defense/2026/04/16/starlink-outage-hit-drone-tests-exposing-pentagons-growing-reliance-on-spacex/>
52. Congressional Research Service, IF12840 (updated 4 September 2025), not accessed: https://www.congress.gov/crs_external_products/IF/PDF/IF12840/IF12840.10.pdf
53. Yahoo News / Reuters, "Musk ordered Starlink shutdown during Ukraine's 2022 Kherson counteroffensive, Reuters reports", July 2025: <https://www.yahoo.com/news/articles/musk-ordered-starlink-shutdown-during-142037065.html>
54. UNITED24 Media, "'I'm safe': Starlink keeps Ukraine's civilians connected as Russia targets the energy grid": <https://united24media.com/life-in-ukraine/im-safe-starlink-keeps-ukraines-civilians-connected-as-russia-targets-the-energy-grid-15559>
55. CircleID (Larry Press), "Starlink in Ukraine: what three years of wartime connectivity taught us", 6 January 2026: <https://circleid.com/posts/starlink-in-ukraine-what-three-years-of-wartime-connectivity-taught-us>
56. Wikipedia, "Telecommunications in Ukraine": https://en.wikipedia.org/wiki/Telecommunications_in_Ukraine
57. Defense Security Cooperation Agency, "Ukraine – Satellite communications services" (Transmittal 25-58), 29 August 2025: <https://www.dsca.mil/Press-Media/Major-Arms-Sales/Article-Display/Article/4290506/ukraine-satellite-communications-services>
58. Euromaidan Press, "Fears that Ukraine will lose Starlink are back after Musk backed Trump against Zelenskyy. Adviser says profit makes cutoff unlikely", 11 October 2026: <https://euromaidanpress.com/2026/10/11/fears-that-ukraine-will-lose-starlink-are-back-after-musk-backed-trump-against-zelenskyy-adviser-says-profit-makes-cutoff-unlikely/>
59. Office of Senator Shaheen, letter to Secretary Austin on commercial provider contracts after the Starlink incident in Ukraine, 15 September 2023: <https://www.shaheen.senate.gov/shaheen-warren-and-duckworth-send-letter-to-secretary-austin-requesting-information-about-defense-contracts-with-commercial-providers-following-the-reported-starlink-incident-in-ukraine>
60. CBS News, "Elizabeth Warren asks about contingency plans amid Trump–Musk feud", 7 June 2025: <https://www.cbsnews.com/amp/colorado/news/elizabeth-warren-contingency-plans-national-security-trump-musk>
61. Kyiv Independent, "US threatens to shut off Starlink if Ukraine won't sign minerals deal, sources tell Reuters", 22 February 2025: <https://kyivindependent.com/us-threatens-to-shut-off-starlink-if-ukraine-wont-sign-minerals-deal-sources-tell-reuters/>
62. DatacenterDynamics, "Trump threatens to cancel SpaceX government contracts amid feud with Musk", 5 June 2025: <https://www.datacenterdynamics.com/en/news/trump-threatens-to-cancel-spacex-government-contracts-amid-feud-with-musk/>
63. Euromaidan Press, "Ukraine wants to aim Starlink at Russian targets and build a version Elon Musk can't switch off", 5 October 2026: <https://euromaidanpress.com/2026/10/05/ukraine-wants-to-aim-starlink-at-russian-targets-and-build-a-version-elon-musk-cant-switch-off/>
64. Washington Technology, "SpaceX's biggest risk factor might be Elon Musk", 21 May 2026: <https://washingtontechnology.com/companies/2026/05/spacexs-biggest-risk-factor-might-be-elon-musk/413698/>
65. South China Morning Post, "China–Singapore security team claims breakthrough in hacking Starlink terminals", 3 September 2026: <https://www.scmp.com/news/china/science/article/3366192/china-singapore-security-team-claims-breakthrough-hacking-starlink-terminals>
66. Kareem, "Cyber threat landscape analysis for Starlink: assessing risks and mitigation strategies", arXiv:2406.07562, 2024: <https://arxiv.org/pdf/2406.07562>
67. Infosecurity Magazine, "Five takeaways from the Russian cyber-attack on Viasat's satellites", May 2023: <https://www.infosecurity-magazine.com/news/takeaways-russian-cyberattack/>
68. Breaking Defense (Valerie Insinna), "SpaceX beating Russian jamming attack was 'eyewatering': DoD official", April 2022 (mailing-list copy): <https://www.metzdwowd.com/pipermail/cryptography/2022-April/037801.html>
69. GlobalSecurity.org, "Starlink: jamming": <https://www.globalsecurity.org/space/world/ukraine/starlink-1.htm>
70. Johns Hopkins Space Security, "The need to protect access points for distant-end users using space-based internet service providers", 8 February 2023: <https://spacesecurity.wse.jhu.edu/2023/02/08/the-need-to-protect-access-points-for-distant-end-users-using-space-based-internet-service-providers>
71. Senetas, "Encrypting Starlink: customer-controlled, quantum-ready protection" (vendor white paper), April 2026: <https://www.senetas.com/wp-content/uploads/Senetas-Encrypting-Starlink-Whitepaper-April2026.pdf>

72. Let's Data Science, "Elon Musk deploys SpaceX engineers to Grok development" (citing Business Insider), 29 June 2026: <https://letsdatascience.com/news/elon-musk-deploys-spacex-engineers-to-grok-development-adf1c236>
73. TeslaNorth, "SpaceX's Starlink rolls out Grok AI chatbot for customer support", 26 September 2025: <https://teslanorth.com/2025/09/26/spacex-starlink-rolls-out-grok-ai-chatbot-for-customer-support/>
74. PiunikaWeb, "Grok-powered voice assistant is handling Starlink customer support calls at SpaceX" (citing PCMag), 15 April 2026: <https://piunikaweb.com/2026/04/15/spacex-grok-voice-ai-starlink-customer-support/>
75. Crypto Briefing, "Starlink uses Grok Voice for 15,000 daily support calls" (via Space.com), 24 August 2026: <https://cryptobriefing.com/starlink-grok-voice-customer-support/>
76. Yahoo Finance / Reuters (David Jeans and Joey Roulette), "Musk's Starlink updates privacy policy to allow consumer data to train AI", 30 January 2026: <https://finance.yahoo.com/news/musks-starlink-updates-privacy-policy-230853500.html>
77. Technext, "Starlink now uses users' data for AI training; here's how to opt out", 2 February 2026: <https://technext24.com/2026/02/02/starlink-now-uses-users-data-ai-training/>
78. Via Satellite, "SpaceX acquires xAI to pursue orbital data center constellation", 2 February 2026: <https://www.satellitetoday.com/connectivity/2026/02/02/spacex-acquires-xai-to-pursue-orbital-data-center-constellation/>
79. Constellation Research, "SpaceXAI launches Grok Bot work assistant", August 2026: <https://www.constellationr.com/insights/news/spacexai-launches-grok-bot-work-assistant>
80. CNBC, "Musk's xAI needs SpaceX deal for the money. Data centers in space are still a dream", 2 February 2026 (headline only, article not accessible): <https://www.cnbc.com/2026/02/02/musks-xai-needs-spacex-for-money-data-centers-in-space-are-a-dream.html>
81. Peled et al. (Ben-Gurion University), "SoK: Evaluating the security of satellite systems", arXiv:2312.01330, December 2023: <https://arxiv.org/pdf/2312.01330>
82. Giuliani, Ciussani, Perrig and Singla (ETH Zurich), "ICARUS: Attacking low Earth orbit satellite networks", probably USENIX ATC 2021 (inferred from the file name, to confirm): <https://netsec.ethz.ch/publications/papers/atc21-final594.pdf>
83. Thummala, Sharma, Calabrese and Falco (Cornell / UNC), "Adversarial machine learning threats to spacecraft", arXiv:2405.08834, 2024: <https://arxiv.org/html/2405.08834v1>
84. Space.com (Tereza Pultarova), "An AI cyberattack could trigger a satellite apocalypse in the next 2 years. Are we prepared?", 19 March 2026: <https://www.space.com/space-exploration/satellites/an-ai-cyberattack-could-trigger-a-satellite-apocalypse-in-the-next-2-years>
85. Cyber Magazine, "AI agents drive first large-scale autonomous cyberattack" (reporting Anthropic's November 2025 report): <https://cybermagazine.com/news/ai-agents-drive-first-large-scale-autonomous-cyberattack>
86. International AI Safety Report 2026 (chair: Yoshua Bengio), 3 February 2026: <https://internationalaisafetyreport.org/publication/international-ai-safety-report-2026>
87. METR, "Frontier Risk Report (February to March 2026)", 19 May 2026: <https://metr.org/blog/2026-05-19-frontier-risk-report/>
88. SatNews, "Elon Musk projects Starlink constellation will deliver majority of global internet traffic within a decade", 23 September 2026: <https://satnews.com/2026/09/23/elon-musk-projects-starlink-constellation-will-deliver-majority-of-global-internet-traffic-within-a-decade/>
89. Teslarati, "SpaceX's newest Starlink will make Earth data centers obsolete", 23 June 2026: <https://www.teslarati.com/spacex-starlink-ai-satellite-vs-starlink/>
90. Next Horizon, "Satellite internet: how Starlink, Amazon Leo, OneWeb and direct-to-cell are building a space-based internet", 2 October 2026: <https://www.nexthorizon.space/2026/10/satellite-internet.html>
91. Iran International, reporting the Wall Street Journal, "Trump administration covertly sent Starlink terminals to Iran", 12 February 2026: <https://www.iranintl.com/en/202602120054>
92. Forbes (Kevin Holden Platt), "SpaceX advance guard joins tech skirmishes to protect Starlink in Iran", 25 March 2026: <https://www.forbes.com/sites/kevinholdenplatt/2026/03/25/spacex-advance-guard-joins-tech-skirmishes-to-protect-starlink-in-iran/>
93. Wikipedia, "United Kingdom involvement in the 2026 Iran war": https://en.wikipedia.org/wiki/United_Kingdom_involvement_in_the_2026_Iran_war
94. CNBC, "Israel hosts wartime visit by Elon Musk, eyes Starlink for Gaza", 27 November 2023: <https://www.cnbc.com/2023/11/27/israel-hosts-wartime-visit-by-elon-musk-eyes-starlink-for-gaza.html>
95. Radio Tamazuj, "Starlink to shut down operations in Sudan" (2024): <https://radiotamazuj.org/en/news/article/starlink-to-shut-down-operations-in-sudan>

96. Carnegie Endowment (Sada), Muhammed Ali Thamer, "Starlink in Yemen: security threat or an opportunity?", 16 January 2025: <https://carnegieendowment.org/sada/2025/01/starlink-in-yemen-security-threat-or-an-opportunity>
97. Gigazine, reporting the Wall Street Journal on black-market Starlink use by Russia and Sudan's RSF, 11 April 2024: https://gigazine.net/gsc_news/en/20240411-starlink-russia-sudan-black-market
98. Defense One, "US military has 'on-orbit' space weapons, Air Force Secretary reveals", 14 September 2026: <https://www.defenseone.com/defense-systems/2026/09/us-military-has-orbit-space-weapons-air-force-secretary-reveals/415964/>
99. CNN, "The US military said it has deployed weapons in space. Here's what that could mean", 15 September 2026: <https://www.cnn.com/2026/09/15/science/us-space-force-weapons-capabilities-hnk>
100. Fortune, "SpaceX, Anduril among companies to win Golden Dome contracts", 25 April 2026: <https://fortune.com/2026/04/25/spacex-anduril-lockheed-raytheon-northrop-golden-dome-interceptor-contracts/>
101. IBTimes UK, "US says its Golden Dome missile-killer is flight-ready, but it is not yet in orbit", 21 September 2026: <https://www.ibtimes.co.uk/us-golden-dome-interceptor-flight-ready-hardware-1821103>
102. CNBC, "SpaceX wins \$4.16 billion Space Force contract for threat-detection satellites", 29 May 2026: <https://www.cnbc.com/2026/05/29/spacex-wins-4point16-billion-space-force-contract-for-threat-detection-satellites.html>
103. European Space Agency, "IRIS² reinforced and accelerated as implementation advances", August 2026: https://www.esa.int/Applications/Connectivity_and_Secure_Communications/IRIS2_reinforced_and_accelerated_a_s_implementation_advances
104. Wikipedia, "Amazon Leo": https://en.wikipedia.org/wiki/Amazon_Leo