



Picture: US Army, https://www.army.mil/article/152664/future_army_nanosatellites_to_empower_soldiers, public domain.

License: Günther Burbach, Free21, CC BY-NC-ND 4.0

By [Günther Burbach](#) | Published on October 28, 2025

Starlink – The silent militarization of the skies

How a private satellite network is changing war, politics, and the atmosphere.

Camouflage as a civilian engineering project

Starlink is often touted as a triumph of modern engineering, a global network of thousands of small satellites designed to provide internet access to even the most remote regions. It promises connectivity and progress, digital equality and technological innovation. But behind this rosy narrative lies a project that has long since transcended the civilian sphere. Starlink is not just a communications infrastructure, but a geopolitical architecture designed to project power, exert control, and secure digital supremacy in orbit.

The official narrative follows a simple pattern: SpaceX as a revolutionary company democratizing the skies. Elon Musk as a visionary bringing the network to where governments fail. In reality, however, the business model is so heavily subsidized that the term "private" hardly applies anymore. More than half of the development costs come from government contracts—military, security-related, classified.

Even more problematic is the structural effect: Starlink is removing global communications infrastructure from public control. What was once subject to national or multilateral rules now

belongs to a US-based company that is neither accountable to international bodies nor subject to democratic regulation. Those who want access pay. Those who are blocked remain silent.

That such a system was designed for strategic dominance from the outset is evident in its architecture. The satellites fly in low Earth orbits, are modularly interchangeable, and can be replaced within days. A "living swarm" that is constantly being expanded, replaced, and optimized. Control lies in automated ground stations whose software is centrally managed via servers in the USA. No state in the world has access to it.

This means that the planetary communication layer is effectively privatized. And this privatization is irreversible as long as no alternative system of comparable range exists. Europe is planning such a counterweight with IRIS², but it is years behind—technologically, financially, and politically.

Starlink is thus a textbook example of modern power politics disguised as digital innovation: a civilian project that has long since fulfilled a strategic function. While governments are still talking about "digitalization," the skies above them are already divided into private zones—a network that regulates itself, renews itself, and no longer serves the purpose it purported to.

Ukraine – the test run

The war in Ukraine was the moment when Starlink revealed its true nature. What had previously been touted as a civilian technology promise—high-speed internet for remote regions—transformed into a military backbone in the spring of 2022. While Russian troops destroyed radio masts, severed fiber optic cables, and the country's communication networks collapsed within hours, small, inconspicuous gray cases—Starlink terminals—suddenly appeared at Ukrainian military bases. They didn't arrive by humanitarian chance, but through official Pentagon channels.

Within a few weeks, several thousand devices were operational. They were located in command posts, field hospitals, and makeshift drone bases. Commands, satellite images, and target data flowed through them. The Ukrainian Ministry of Defense spoke of a "communicative resurrection." What hardly anyone noticed: This lifeline didn't run through Ukrainian infrastructure, but through a private network owned by the United States.

Starlink didn't just enable communication between units. It changed warfare itself.

Drone pilots could control their devices in real time over hundreds of kilometers, artillery officers received precise target coordinates from the cloud, and medics transmitted live images from front lines. The speed at which information flowed was militarily revolutionary and politically sensitive. Because it depended on a single man: Elon Musk.

In September 2022, a crisis erupted. The Starlink connection was not activated in parts of Crimea, for fear that Ukraine might use the system to attack Russian positions and thus "draw them into a world war." Suddenly, entire drone squadrons were without signal. In a modern war, where communication means life, this was a tactical earthquake.

This moment revealed the new reality: A private entrepreneur was deciding the fate of a sovereign state's military operations. No general, no defense secretary, no president—a single technology company controlled the communication arteries of an army. The Pentagon reacted with a mixture of admiration and panic. Admiration because the system was so robust and effective. Panic ensued because it wasn't state-owned.

Since then, Washington has been trying to secure its influence through contractual agreements. But the precedent remains: For the first time in the history of warfare, a private network became both a crucial tactical instrument and a political risk.

Starlink wasn't an aid project in Ukraine. It was a test run. A demonstration of how technology can shift power: away from states and toward corporations. And this test run was so successful that military integration is now merely a matter of formal implementation.

Military Integration – Starshield and the New Orbital War

After the Ukraine deployment, it was clear: Starlink was no longer just civilian infrastructure; it was military infrastructure, just privately operated. And barely a year later, this realization became an official program. In December 2022, SpaceX announced a new brand: Starshield. The name was no coincidence. It represented the next step: the integration of the private satellite constellation into the United States' military architecture.

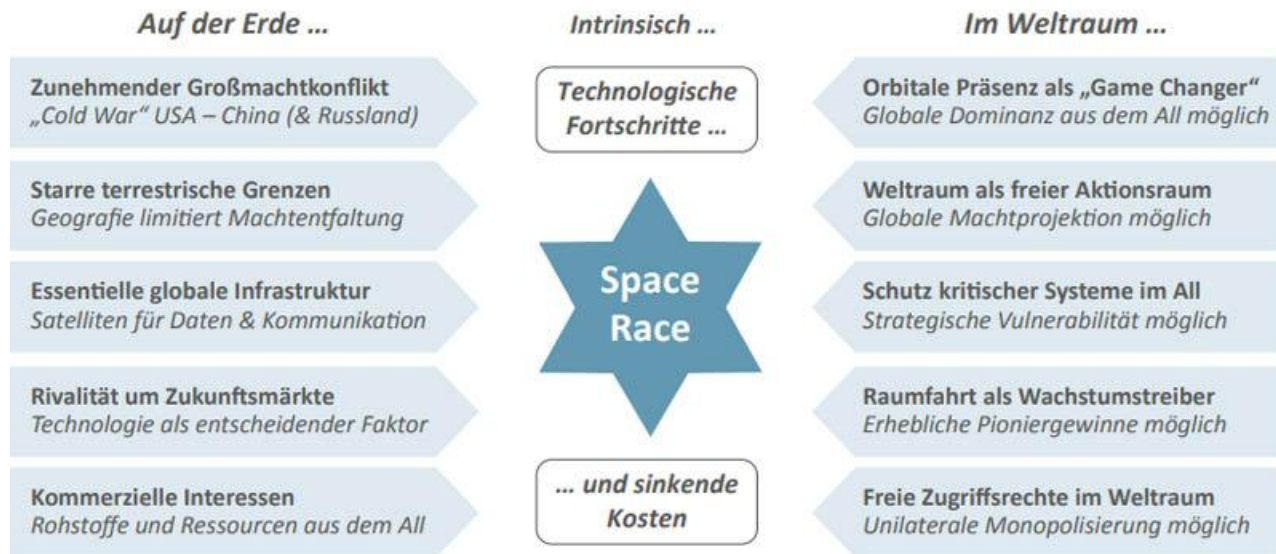
Starshield is technically almost identical to Starlink, but the software and prioritization differ fundamentally. While Starlink was developed for civilian users, Starshield operates with military encryption protocols, tiered access levels, and exclusive data channels for the Pentagon. In official documents from the US Space Development Agency (SDA), the system is described as a "flexible, scalable communications network for tactical operations." The underlying idea is simple: if warfare is digital, the network must not be publicly owned, but rather secure. And "secure" in this case means: American.

The Pentagon has massively expanded the cooperation since 2023. Starshield is being tested for real-time communication between drone swarms, for data transmission between reconnaissance satellites, and for integration with AI-supported targeting systems. It is part of the "Joint All-Domain Command and Control" (JADC2) concept, which aims to unify the flow of information between land, air, sea, cyber, and space operations. In other words:

Starlink and Starshield form the backbone of the digital command level for future wars.

While governments are still debating data privacy and arms control, the US military is creating its own redundant communications sphere. And it's no longer on Earth, but in orbit. The US no longer needs terrestrial infrastructure to coordinate its armed forces; it has a private cloud made of aluminum, solar cells, and radio frequencies that operates globally.

Abb. 2: Wichtige Treiber der Dynamik im neuen Space Race



Source: FERI Cognitive Finance Institute, 2024, “Space Cold War”: Massive Militarization of Space as a Global Risk, https://www.feri-institut.de/media/eudl4obq/feri_cfi_cc_space_2406120.pdf

But the consequences extend far beyond military efficiency. The introduction of Starshield is creating an entirely new sector: commercialized space warfare. This is an area where companies fulfill defense contracts but retain physical control over the system. SpaceX remains the owner of the satellites, even when they are operating for the Pentagon. This is legally novel and politically explosive. In a crisis, it would be unclear who decides on deployment, shutdown, or target prioritization—the state or the operator.

Other nations are also working on similar models: China with its "Guowang" constellation, Russia with "Sfera." The result is a global arms race in orbit—a "Space Race 2.0," this time not between states, but between military-commercial networks.

Starshield demonstrates where this is headed: Space is no longer neutral territory, but a militarized data zone. The sky above us is no longer empty; it is filled with systems that listen, see, transmit, and make decisions. And they do not belong to humanity, but to those who control them through contracts, software, and capital.

The geopolitical lever

Starlink is far more than just a technical system; it's a geopolitical tool. Whoever controls a country's communications infrastructure also controls its room for maneuver. And that's precisely what's happening—not openly, not aggressively, but insidiously, under the guise of digitalization.

With Starlink, the US has created an instrument that goes far beyond traditional diplomacy or military presence. It's a tool of strategic dependency. States that allow the network become part of an American-dominated data architecture. States that block it have to build their own alternatives, which costs years and billions. This isn't theory, but visible practice: African countries that have opened up to Starlink can now be connected within days, but the entire technical infrastructure, from orbit to the ground, remains proprietary to the US. No state, no telecommunications provider, no international regulator can track what's happening on these channels.

This asymmetric dependency is highly effective geopolitically. Starlink is essentially the first digital equivalent of US aircraft carriers: mobile, deployable anywhere, difficult to attack, and activatable at any time. Where infrastructure previously had to be built, protected, or destroyed, a signal from orbit is now sufficient. A single button press can connect entire regions to the network or disconnect them.

For Washington, this is a strategic dream. Starlink enables what traditional alliance politics often cannot: control without direct occupation. Military presence is replaced by digital presence, national sovereignty by licensing rights. And all of this happens legally, based on commercial agreements.

China and Russia have long recognized the implications. Both are working on alternative models:

- China is building its own mega-constellation with over 12,000 satellites under the name „**Guowang**“ (国网, „National Network“),
- Russia is responding with the "**Sfera**" project, which aims to link civil and military services. Both systems are intended to technologically mirror Starlink, but will remain under state control.

Europa hingegen hat geschlafen.

Das Projekt **IRIS²**, das bis 2027 ein eigenständiges europäisches Satellitennetz aufbauen soll, kommt kaum voran. Budgetkürzungen, Kompetenzstreitigkeiten und eine politische Naivität gegenüber der Geschwindigkeit privater Akteure machen die EU zu einem digitalen Zaungast. Während Brüssel Datenschutzverordnungen schreibt, erobern US-Konzerne den Orbit.



The European Union is attempting to establish an independent satellite network with IRIS2, which is intended to increase security and connectivity. (Image: European Commission, screenshot from 16 October 2025: https://defence-industry-space.ec.europa.eu/eu-space/iris2-secure-connectivity_en)

The geopolitical consequence is clear: Whoever operates Starlink possesses not only data sovereignty, but also the power to exert influence. The line between digital sovereignty and de facto foreign control is becoming blurred. A country that conducts its communication via a foreign network is no longer a sovereign nation; it is a technological protectorate.

Starlink has united the West, but divided the rest of the world. For many countries, it is both a blessing and a threat: access to the network in exchange for relinquishing control. And therein lies the geopolitical leverage—subtle, inconspicuous, but more effective than any sanction.

Dependency as a system

Ukraine was the experiment, Starshield the prototype, but the real goal lies beyond that: a global communications network that can be selectively controlled in times of crisis or conflict. What initially sounds like a technological vision has long since become reality. Starlink has created a new form of dependency—invisible and quiet, but structurally profound.

This dependency operates on several levels. **First, technologically:** once connected to Starlink, there's virtually no way back. The terminals, the software, the frequencies—everything is proprietary, encrypted, and closed. Even governments that officially approve the system have no access to its controls. If SpaceX decides to shut down a region, it goes dark. No law, no treaty can prevent this. What once meant sovereignty—control over one's own communications infrastructure—is, in this model, tied to private keys.

The second level is **economic**. Starlink is not just a network, but a global subscription system. Those who are part of the system pay and thus remain permanently trapped in a cycle of digital dependency. States that use Starlink as their national communications platform invest millions in terminals, licenses, and support. But they don't own any of it. They are leasing their own connection to the world. This is no longer a classic commercial relationship, but rather a structural form of technological blackmail.

Finally, there is the **political level**. Starlink operates as "private infrastructure," but with direct access to military decision-making structures. The US government can contractually mandate priorities without other states having insight. This structure makes the network an instrument of political control—subtle, but effective. If a country acts against US interests, theoretically, restricting data flow is enough to generate economic and social pressure.

The emerging concept is new: digital hegemony through infrastructure control. Not weapons, but frequencies determine power. Not columns of tanks, but server farms.

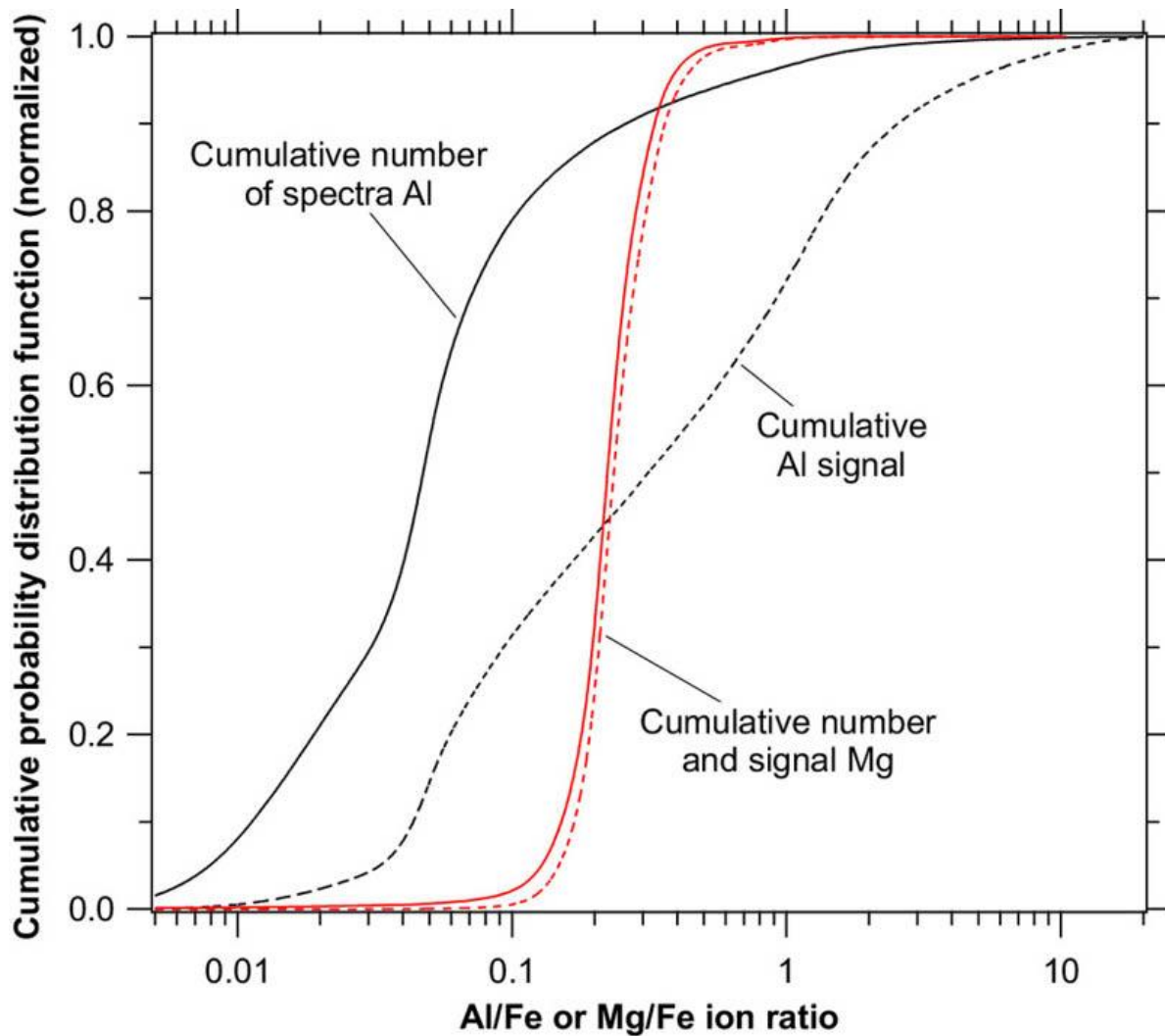
This dependency is intentional. It is not collateral damage of innovation, but its very purpose. Starlink and similar systems are designed not only to connect countries, but to bind them to the Western technological order. It is a form of modern vassalage, encoded in data packets and terms of service.

And this logic is irreversible. Once someone has become part of the network, they cannot leave without regressing. This is the new principle of global control: not ownership, but access determines power, and whoever grants access sets the rules.

The ecological shadow

While Starlink's political and military influence is steadily growing, its environmental impact is almost entirely ignored. Yet it is enormous. This seemingly invisible infrastructure in space comes at a very real ecological cost, and that cost increases with every new satellite launch.

It starts with production: Each Starlink satellite weighs approximately 260 kilograms and consists primarily of aluminum, silicon, rare earth elements, copper, and lithium. Its manufacture requires around 20 to 25 megawatt-hours of energy, as well as highly specialized production processes under cleanroom conditions. This translates to an enormous carbon footprint long before the satellite even launches. With over 6,000 units in orbit and thousands more in the planning stages, this results in a gigantic material balance—a cycle of melting, launching, and incineration.



Cumulative probability distributions of the Al and Mg ion signals for particles containing Fe during all SABRE 2023 flights from Alaska ($n \approx 175,000$). Particles with an Al/Fe ratio greater than 0.1 are likely influenced by spaceflight and account for more than 20% of the particles containing metals. These Al-enriched particles contain about 70% of the cumulative aluminum signal (dashed line). The Mg/Fe distribution is much narrower than the Al/Fe distribution because meteorites are the dominant source of Mg and Fe. (Graphic: D.M. Murphy, M. Abou-Ghanem, D.J. Czicz, K.D. Froyd, J. Jacquot, M.J. Lawler, C. Maloney, J.M.C. Plane, M.N. Ross, G.P. Schill, & X. Shen, Metals from spacecraft reentry in stratospheric aerosol particles, *Proc. Natl. Acad. Sci. U.S.A.* 120 (43) e2313374120, <https://doi.org/10.1073/pnas.2313374120> (2023))

Each of these satellites has a lifespan of only about five years. After that, it is deorbited in a controlled manner and burns up in the atmosphere. What sounds like a clean recycling process is, in reality, a large-scale release of metal oxides. Upon re-entry, the aluminum oxidizes into fine dust, aluminum oxide, which remains in the mesosphere and stratosphere. Studies by the University of British Columbia and the US National Oceanic and Atmospheric Administration (NOAA) show that several hundred tons of this material are already released into the upper atmosphere annually. With the planned constellations, this could amount to several thousand tons per year by 2030.

These particles are not harmless. Aluminum oxide is chemically stable and reflects ultraviolet light. In large quantities, it alters the atmosphere's radiation balance, similar to soot particles or sulfates. In the long term, this could influence the temperature distribution in the upper atmosphere, and perhaps even processes in the ozone layer. No one yet knows exactly how this new, man-made carbon cycle in the sky will play out, but its impact is undeniable.

Added to this is the energy consumption of rocket launches. A single Falcon 9 rocket burns about 112 tons of kerosene (RP-1) and emits around 350 tons of CO₂. In 2024 alone, SpaceX launched over 100 times, generating more than 35,000 tons of CO₂ emissions, just for the transport of new satellites. These emissions are released directly into the upper atmosphere, where they have a different climatic effect than at ground level. They contribute to warming but can also cause local cold anomalies.

Then there is the debris aspect: Some of the burning satellites do not reach the ground completely destroyed. Metal fragments, especially those made of heat-resistant alloys, survive reentry and land, often unnoticed, in oceans or remote regions. NASA regularly documents such cases. With each day that several satellites burn up in the atmosphere, the total mass of material entering the global biogeochemical cycle increases.

Starlink is therefore not just a digital network, but also a physical system with a planetary footprint. Every message that travels through the network leaves a trail of energy, aluminum, and kerosene in its wake. And the larger the constellation grows, the more invisible the ecological cost becomes, because it has literally been shifted to the skies.

The space industry speaks of "sustainable connectivity." In reality, it is the opposite: a permanently rotating cycle of production, launch, use, and destruction—a high-tech consumption system that transforms the skies into a dumping ground.

The new form of power

Starlink marks the transition to a new era of political and technological power. It is the first system to demonstrate how sovereignty is being redefined in the digital world, no longer through territory or weapons, but through control over networks, data, and infrastructures that are not subject to any constitution. Here, the state is not gradually losing its central function—the protection of communications sovereignty—but rather openly.

Previously, only states could operate global communication networks: submarine cables, radio frequencies, satellites. Today, however, private corporations control systems that can connect or disconnect entire countries in real time. Starlink is merely the most visible example of a development that extends far beyond orbit: Amazon with Kuiper, OneWeb with British-Indian capital, China with Guowang. But no other system is as large, has grown as rapidly, and is as deeply integrated into military processes as the SpaceX network.

This fundamentally shifts the balance of power. The new form of authority is no longer based on state legitimacy, but on technological superiority. One could say: The monopoly of force is being replaced by the monopoly of infrastructure. And this monopoly is far more effective because it is barely visible.

Starlink operates outside traditional legal frameworks. It is not subject to international law, UN regulations, or clear liability. The satellites fly in low Earth orbits, moving between national airspace and the global vacuum—a legal no-man's-land. If a country were affected by a shutdown or manipulation, there would be no authority that could demand compensation. Even if a state opposes its use, like Russia or China, it cannot technically prevent it without militarily contesting the orbit.

This creates a new form of power: technological sovereignty without political responsibility. This is the real revolution that Starlink has ushered in.

The ability to create, move, or delete communication spaces is more valuable today than any army.

Because whoever controls what people see, hear, or transmit also controls their worldview. And this power is not hypothetical. It is already being used:

- in Ukraine, where Starlink decides on military operations,
- in Africa, where governments are digitally leasing entire regions,
- in the USA itself, where the system is part of national security strategies.

What is emerging here is a digital feudalism, a world in which corporations rule communication territories like princes, while states become vassals of their own infrastructure. They pay for access, but they don't own it. They may use it, but not shape it. They have responsibility without control. This is not a dystopian future, but the present. Starlink has shown how quickly power can shift when mediated by technology. And it has created a blueprint that others will follow: private actors overtaking states, not because they are stronger, but because they act faster, more globally, and with less accountability.

Conclusion – The sky as a new limit of power

Starlink is not a communications network in the classical sense. It is an instrument of power, precisely engineered, strategically deployed, and politically underestimated. What began as a technological innovation has become a system that places states, armies, and entire societies in a state of digital dependency. It is the logical product of a world order in which capital, technology, and security merge.

The sky, once a symbol of human freedom, is now the invisible boundary of a new kind of domination. Whoever controls it controls the Earth. And this no longer happens through military occupation, but through orbital infrastructure. Power no longer resides on the battlefields, but in networks, algorithms, and frequencies.

Starlink thus embodies a new form of imperial expansion: no colonies, no borders, no flags, just a grid of data that overlays the Earth like a second atmosphere. This form of dominance is more

subtle, but also more comprehensive. It can simultaneously connect and subjugate, network and isolate. Control lies with a few actors who operate globally but are accountable to no one. They are not elected, not vetted, not accountable, and that is precisely what makes them dangerous.

At a time when nations are grappling with climate goals and data privacy, a new power structure is establishing itself above their heads, operating outside any constitution. Starlink is the first stage of this development. Others will follow: Amazon with Kuiper, China with Guowang, and perhaps soon, militarily networked AI systems autonomously monitoring entire regions.

If there is no political counter-movement, the future will be shaped not by governments, but by infrastructures; not by decisions, but by networks; not by democratic control, but by technological efficiency.

The skies have thus become the new front line, not of war in the old sense, but of sovereignty. Whoever controls them controls humanity's communication arteries. And whoever controls them writes history. Starlink is the beginning of this story. How it ends depends on whether the world recognizes that the greatest threat does not come from above, but from its own complacency in placing power in the hands of those least accountable.



Author: [Günther Burbach](#)

Günther Burbach is a metalworker and welder who subsequently trained as an IT specialist. After years in steel construction, Burbach worked as an IT specialist, including at Telekom. He writes for publications such as Lokalkompass, part of the Funke Media Group.

Sources:

- Washington Post (Correction & Explanation, Sept. 8/13, 2023)
“Correction: Musk did not shut down the service; coverage was not activated up to 100 km from Crimea, Ukraine requested activation, which was refused” (incl. interview/video with Isaacson).
<<https://www.washingtonpost.com/world/2023/09/08/elon-musk-starlink-ukraine-war>>
- Walter Isaacson – Public Clarification (X/Twitter, Sept. 9, 2023)
- “The Ukrainians thought the coverage extended to Crimea; they asked Musk to activate it – he didn’t...”, <<https://x.com/WalterIsaacson/status/1700342242290901361>>

- Reuters investigation (July 25, 2025) – separate allegation of a regional blackout in occupied territories (Kherson, etc.) at the end of September 2022; SpaceX denies parts of it. A separate issue, clearly distinct from the Crimea episode.
<<https://www.reuters.com/investigations/musk-ordered-shutdown-starlink-satellite-service-ukraine-retook-territory-russia-2025-07-25/0>> Starshield / military integration – demonstrably verifiable
- Official SpaceX website (Starshield, public since Dec. 2022),
<<https://www.spacex.com/starshield/>>
- Reuters Exclusive (March 16, 2024) – Classified NRO contract (~\$1.8 billion) for reconnaissance/spy satellite network (hundreds of satellites),
<<https://www.reuters.com/technology/space/musks-spacex-is-building-spy-satellite-network-us-intelligence-agency-sources-2024-03-16/>>

Environment/Atmosphere (Aluminum Oxide/Particles, Ozone) – Peer Review & Authorities

- PNAS (Murphy et al., NOAA, 2023) – Measurements: Metals from spacecraft reentry in stratospheric aerosol particles,
<<https://www.pnas.org/doi/10.1073/pnas.2313374120>>
- NOAA/CIRES (2025) – Scenarios: Within 15 years, plummeting satellites could release enough aluminum oxide to alter winds & temperatures in stratosphere NOAA-CSL:
<https://csl.noaa.gov/news/2025/427_0428.html>
- FCC – Press & Order (Sept. 29/30, 2022) – binding 5-year rule for LEO satellites after mission end (instead of 25 years), <<https://www.fcc.gov/document/fcc-adopts-new-5-year-rule-deorbiting-satellites>>
- Reuters (April 4, 2025) – Germany/EU promote alternatives (Eutelsat/OneWeb) due to dependence on Starlink, <<https://www.reuters.com/business/media-telecom/germany-funds-eutelsat-internet-ukraine-musk-tensions-rise-2025-04-04>>
- **WELT (2022–23)** – military benefits/dependency, Crimea episodes (see above),
<<https://www.welt.de/241304403>>