



A REGULATORY PERSPECTIVE

From Coverage to Continuity

Space as a resilience layer for disaster risk management

COMMUNICATIONS REGULATORY AUTHORITY
OF THE REPUBLIC OF LITHUANIA

Satellite-based Services for Disaster Risk Management | Vilnius, 1 October 2026

AUGUST 2026 STORM

When the power went out, connectivity went with it

One weekend storm left hundreds of thousands of households without electricity — and mobile sites with them

~800

mobile base stations off the network within a few hours

~70,000

customers left without communication services

100,000s

more experienced degraded service



What the public debate was about

Generators

Alternative communication paths were not part of the conversation

This is not a technology gap. It is an awareness and preparedness gap, at every level

Satellite is an additional path — prepared before the crisis, not improvised during it

Coverage is not continuity

Lithuania is highly connected. A disaster tests something else

99.72%

5G household coverage

69.1%

households with ≥ 100 Mb/s mobile potential

23.5%

rural households with ≥ 100 Mb/s mobile potential

ALREADY IN PLACE

Backup power from 2028

≥ 2 h access & distribution, ≥ 24 h core

2026 spectrum auction obligations

100 Mb/s to 95% of white-zone households by end-2028; all settlements > 200 people by 2030

Crisis obligations

National roaming and priority communications in emergencies

AVAILABILITY

Is there a signal?

QUALITY

Is the service good enough — also in rural areas?

CONTINUITY

What still works when power, backhaul or sites fail?

Coverage is a prerequisite for resilience. It is not resilience itself

Start with the service that must survive

In a crisis, "always connected" means a guaranteed minimum — not normal quality

PEOPLE

- Warnings
- Emergency calls and requests for help
- Trusted information

RESPONDERS

- Operational communications
- Location and situational data
- Coordination across services

INSTITUTIONS

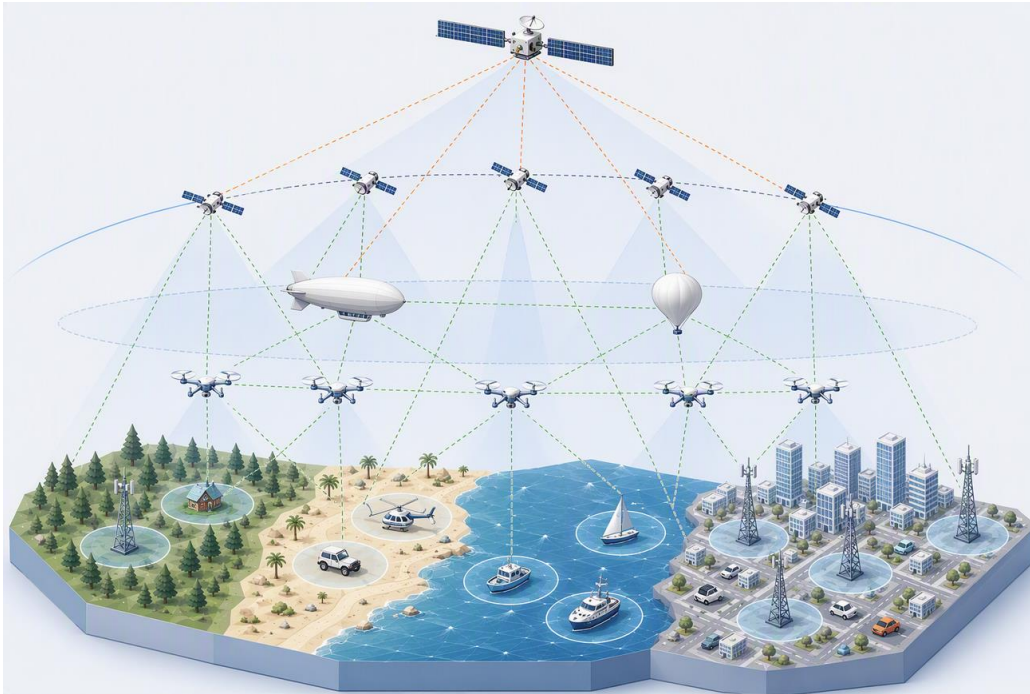
- Command and control
- Secure government communications
- Critical infrastructure coordination

DEFINE FIRST priority users • minimum service • locations • autonomy period • activation authority

The first question is not which technology. It is which service must survive

No single network is resilient alone

Different layers fail in different ways. That is exactly why they work together



SPACE

LEO / MEO / GEO

Wide-area reach, independent of damage on the ground

HIGH-ALTITUDE

HAPS

Persistent regional coverage

AERIAL & DEPLOYABLE

Drones, portable cells

Rapid local restoration

TERRESTRIAL

Mobile, fibre

The backbone: capacity, low latency, indoor and outdoor service

! Different bands, one shared weak point: most layers rely on GNSS signals for time and position

Resilience comes from complementary layers — without a common point of failure

Options exist. The rules are being set now

Use what is available, build the European option, shape the international framework

AVAILABLE NOW

Commercial LEO

Fast and proven — but a single non-EU provider

EMERGING

GOVSATCOM

Secure governmental links

EUROPEAN FUTURE

IRIS² • EUCCS • D2D

Sovereign, secure and cross-border capability, satellite messaging to ordinary phones

DECISIONS AHEAD

ITU PP-26 Nov 2026

Resilient connectivity and stronger action on harmful interference

ITU WRC-27 2027

A real international framework for direct-to-device
New spectrum for different applications

EU / CEPT now

D2D coexistence rules and a common EU position

Use what exists. Build the European option. Shape the rules now

Emerging risk for Europe: GNSS interference

It hits terrestrial and satellite services alike — and stops at no border

OVER LITHUANIA

3 → 40

GNSS spoofing sources in 18 months

~80%

of flights affected daily (August 2026)

The rules exist. Enforcement does not

ENFORCE

One European voice at ITU, ICAO and IMO — with real consequences

STANDARDISE

A common resilience baseline for terrestrial and satellite equipment

PROVE

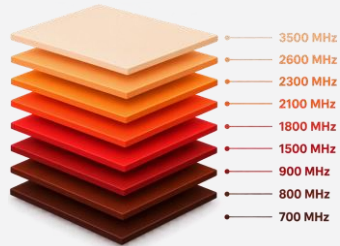
Validate it on Lithuania's live, open interference data

Resilience must be built into the standard — not added after the attack

Crisis-priority network: a case to test in Lithuania

An illustrative RRT planning scenario: sites and spectrum in peacetime, in crisis, and with a satellite layer

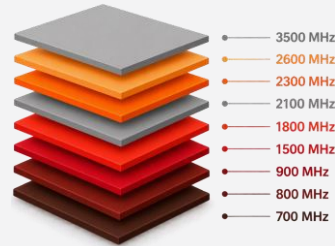
01 PEACETIME



≈6,000 sites

All bands in use: capacity and quality

02 CRISIS PRIORITY



≈1,500 sites

Basic mode: grey bands not in use

03 SATELLITE D2D / D2C



A trusted layer where terrestrial service is unavailable



2100 MHz (mobile band)

Suited to satellite; trial band to be agreed

Controlled, not automatic. Pre-authorized • technically bounded • monitored • coordinated with neighbours • reversible

Our proposal: test it in Lithuania — to find where satellite adds measurable value

The regulator's role: enable, protect, prepare

Lithuania can test continuity, not only connectivity



ENABLE

- Experimental spectrum sandbox
- Radio frequency trading platform
- D2D and satellite trials in real conditions



PROTECT

- Continuous spectrum monitoring: baseline and live picture
- GNSS resilience laboratory with open data
- Cross-border coordination



PREPARE

- Minimum-service and priority rules
- Crisis activation procedures
- Joint exercises and stress tests

HOW A LITHUANIAN TESTBED WOULD WORK

1 DEFINE

crisis scenario, users, minimum service

2 AUTHORISE

temporary, conditional, reversible

3 MEASURE

coverage, delivery, interference

4 PROTECT

active networks and neighbours

5 LEARN

evidence for CEPT, EU, ITU

Regulators do not build constellations. We build the conditions for trustworthy continuity

Resilience is built before disruption

Terrestrial backbone
+ trusted satellite layer
+ prepared users
+ tested procedures



Connectivity everywhere, for everyone, always.