The University of Texas at Austin

THE UNIVERSITY OF TEXAS AT AUSTIN RADIONAVIGATION LABORATORY

Civil PNT Threats and Countermeasures

Todd Humphreys

The University of Texas at Austin

CGSIC | September 17, 2024

Spillover

THE UNIVERSITY OF TEXAS AT AUSTIN
RADIONAVIGATION LABORATORY

Electronic warfare (EW) has historically been a highly classified topic. But its recent spillover effects on civil systems far from any battlefield demand more open discussion and research on the topic.

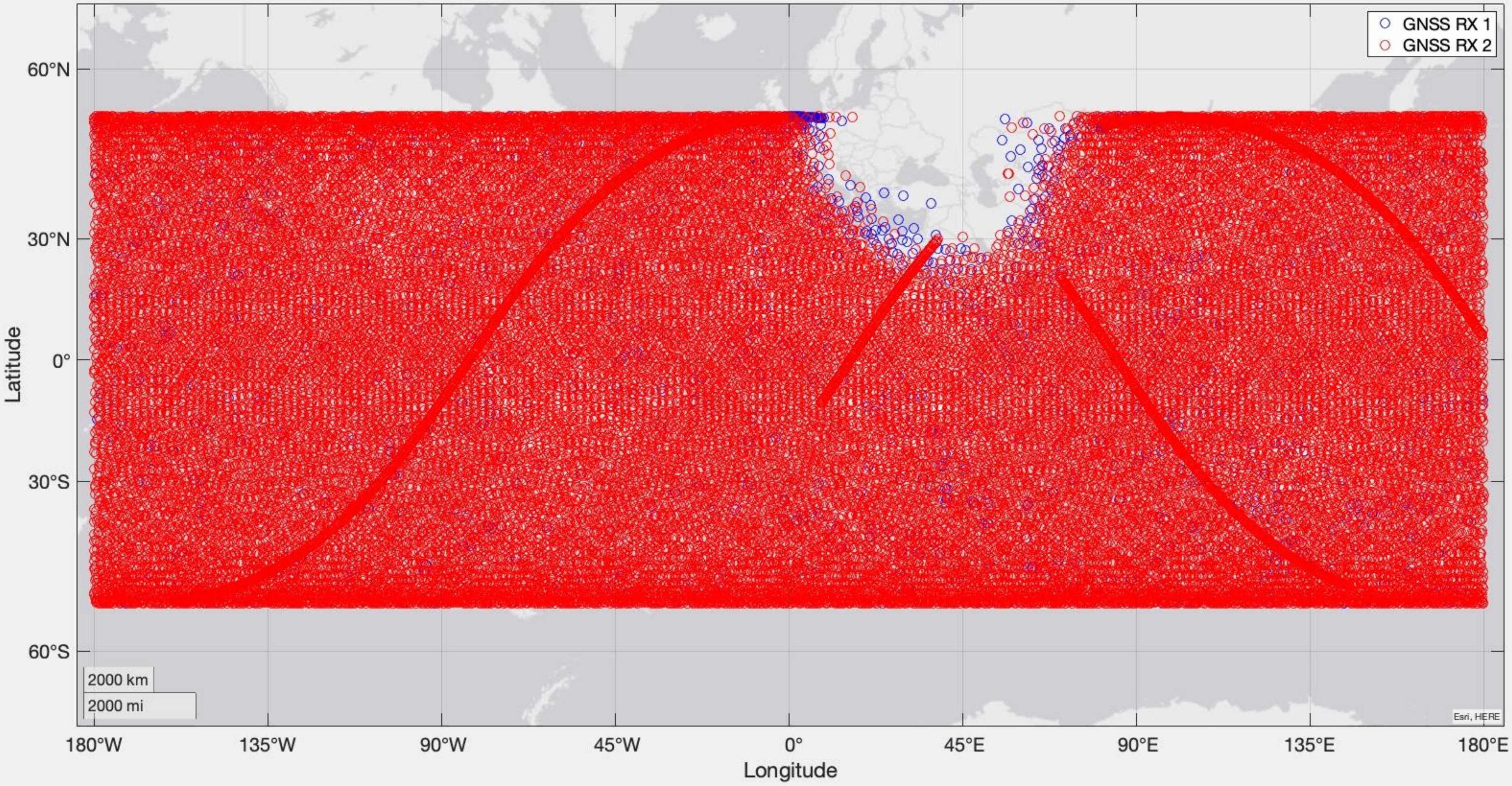
GPSJAM
Daily maps of GPS interference
About | FAQ
02/23/2022
More
Search for a place
Projection
Globe
Level of GPS interference
Low 0-2%
Medium 2-10%
High > 10%
mapbox
Data provided by adsbexchange.com
© Mapbox © OpenStreetMap Improve this map
Greenland
Svalbard
Barents Sea
Iceland
Russia
Sweden
Norway
Finland
North Atlantic Ocean
Ireland
Denmark
Estonia
Latvia
Lithuania
Netherlands
Germany
Poland
Belarus
Moscow
France
Czechia
Ukraine
Switzerland
Austria
Slovakia
Spain
Croatia
Romania
Italy
Bulgaria
Black Sea
Georgia
Armenia
Greece
Turkey
Syria
Cyprus
Israel
Iraq
Iran
Kazakhstan
Kyrgyzstan
Uzbekistan
Tajikistan
Turkmenistan
Afghanistan
Pakistan
India
Mongolia
China
Nepal
Morocco
Algeria
Tunisia
Libya
Egypt
Saudi Arabia
Kuwait
United Arab Emirates
Yemen
Mauritania
Mali
Niger
Chad
Nigeria
Sudan
South Sudan
Eritrea
Ethiopia
Somalia
Cameroon
Central African Republic
Arabian Sea
Sri Lanka
Maldives

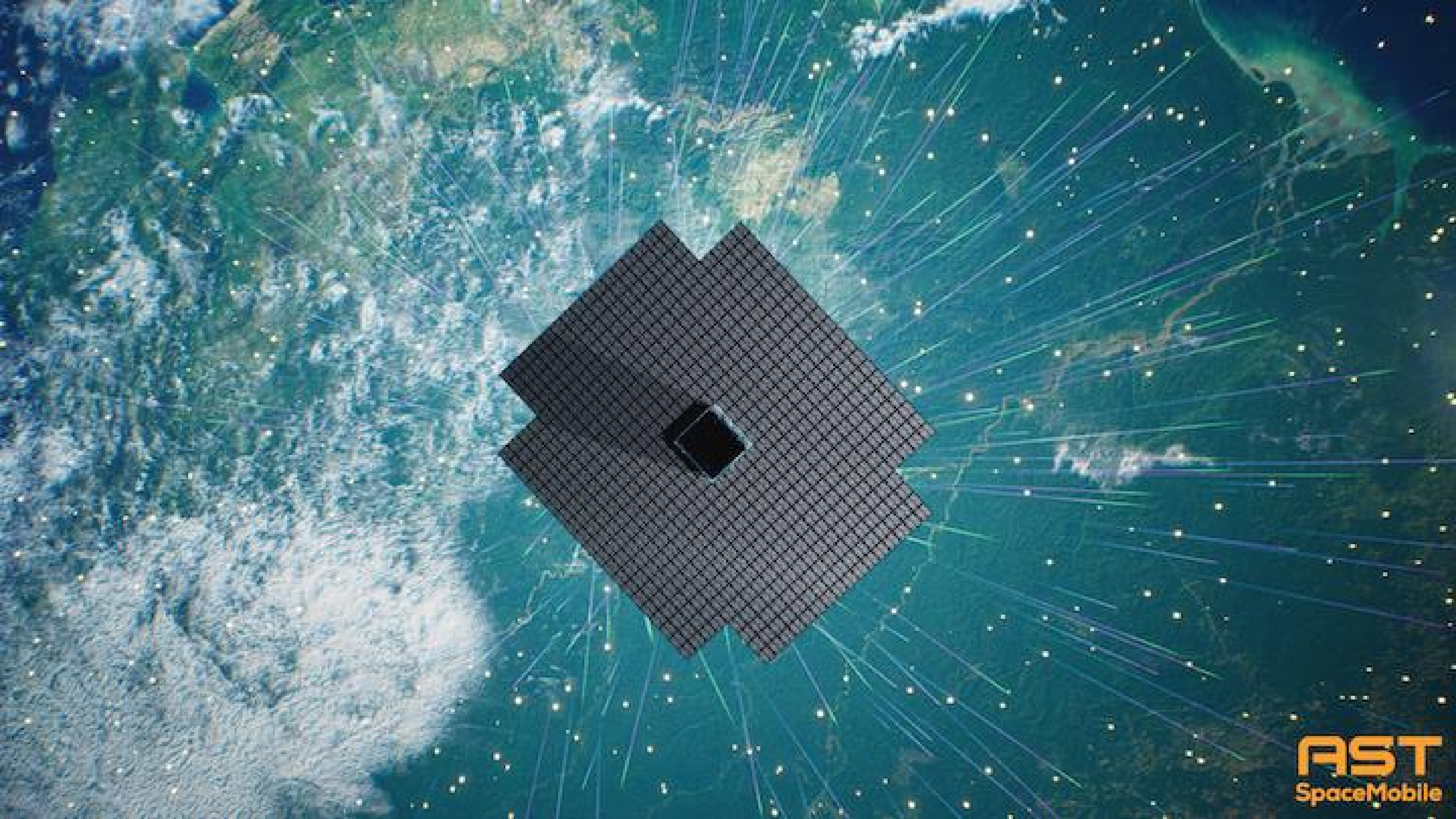

GPSJAM
Daily maps of GPS interference
About | FAQ
03/22/2022
More
Search for a place
Projection
Globe
Level of GPS interference
Low 0-2%
Medium 2-10%
High > 10%
mapbox
Data provided by adsbexchange.com
© Mapbox © OpenStreetMap Improve this map
Greenland
Svalbard
Barents Sea
Iceland
Russia
Sweden
Norway
Finland
North Atlantic Ocean
Ireland
Denmark
Estonia
Latvia
Lithuania
Netherlands
Germany
Poland
Belarus
France
Czechia
Ukraine
Kazakhstan
Mongolia
China
Spain
Switzerland
Austria
Slovakia
Croatia
Romania
Bosnia and Herzegovina
Italy
Bulgaria
Black Sea
Georgia
Armenia
Kyrgyzstan
Uzbekistan
Tajikistan
Turkmenistan
Afghanistan
Nepal
Morocco
Algeria
Tunisia
Greece
Turkey
Cyprus
Syria
Iraq
Iran
Pakistan
India
Israel
Libya
Egypt
Kuwait
United Arab Emirates
Saudi Arabia
Mauritania
Mali
Niger
Chad
Nigeria
Sudan
Yemen
Eritrea
Djibouti
Ethiopia
Somalia
South Sudan
Central African Republic
Cameroon
Sri Lanka
Maldives
Arabian Sea
Moscow
Istanbul
Cairo
Baku
Tehran
Muscat


GPSJAM
Daily maps of GPS interference
About | FAQ
03/01/2024
More
Level of GPS interference
Low 0-2%
Medium 2-10%
High > 10%
mapbox
Data provided by adsbexchange.com
© Mapbox © OpenStreetMap Improve this map
Greenland
Svalbard
Barents Sea
Iceland
North Atlantic Ocean
Russia
Sweden
Norway
Finland
Ireland
Denmark
Estonia
Latvia
Lithuania
Netherlands
Germany
Poland
Belarus
France
Czechia
Switzerland
Austria
Slovakia
Ukraine
Spain
Croatia
Bosnia and Herzegovina
Romania
Italy
Bulgaria
Albania
Greece
Black Sea
Georgia
Armenia
Turkey
Cyprus
Syria
Israel
Iraq
Iran
Kuwait
Saudi Arabia
United Arab Emirates
Yemen
Kazakhstan
Uzbekistan
Turkmenistan
Tajikistan
Kyrgyzstan
Afghanistan
Pakistan
India
Nepal
Mongolia
China
Morocco
Algeria
Tunisia
Libya
Egypt
Mauritania
Mali
Niger
Chad
Sudan
South Sudan
Nigeria
Cameroon
Ethiopia
Somalia
Eritrea
Djibouti
Arabian Sea
Sri Lanka
Maldives
Western Sahara
Central African Republic

September 2023, **First clear case of GPS spoofing of commercial aircraft:**

“Further, the IRS didn’t work anymore. We only realized there was an issue because the autopilot started turning to the left and right, so it was obvious that something was wrong. After couple of minutes we got error messages on our FMS [flight management system] regarding GPS, etc. So we had to request radar vectors. We were showing about 80 nm off track. During the event, we nearly entered Iran airspace (OIIX/Tehran FIR) with no clearance.”


GNSS RX 1
GNSS RX 2
60°N
30°N
0°
30°S
60°S
Latitude
180°W
135°W
90°W
45°W
0°
45°E
90°E
135°E
180°E
Longitude
2000 km
2000 mi
Esri, HERE


AST
SpaceMobile

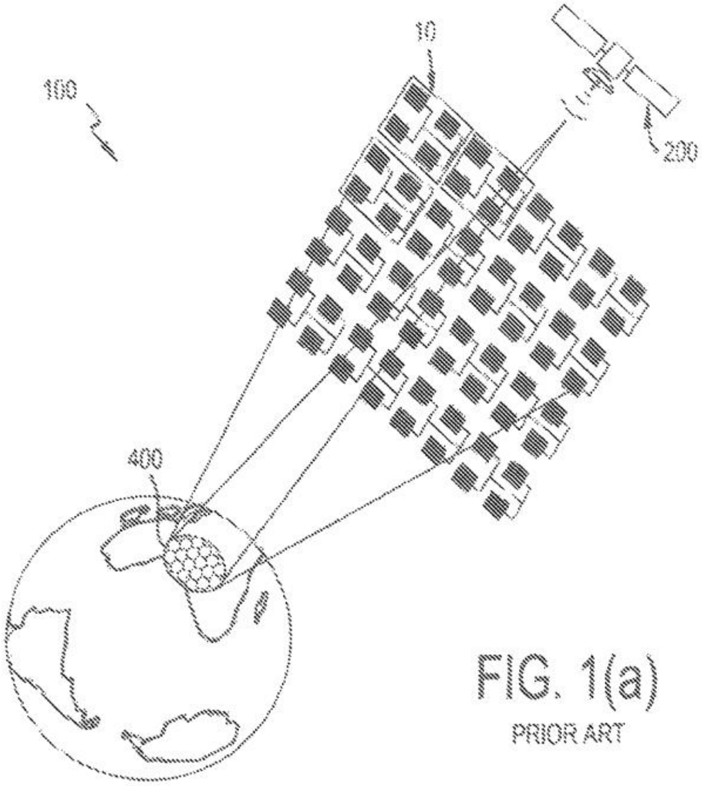


FIG. 1(a)
PRIOR ART

In response to the alarming recent uptick in GNSS jamming and spoofing, and the dangers this poses for civil aviation, the ITU World Radio Conference passed a resolution in December 2023 to emphasize the protected status of the GNSS L1 and L5 bands.

But it was not possible to get agreement on the resolution without introduction of an caveat that, ironically, *weakens* protections of these bands.

RESOLUTION 676 (WRC-23)

Prevention and mitigation of harmful interference to the radionavigation-satellite service in the frequency bands 1 164-1 215 MHz and 1 559-1 610 MHz

The World Radiocommunication Conference (Dubai, 2023),

considering

a) that the radionavigation-satellite service (RNSS) in the frequency bands 1 164-1 215 MHz and 1 559-1 610 MHz is used in several aeronautical and maritime communication, navigation and surveillance safety-of-life systems;

b) that the RNSS is used for safety-of-life applications, for scientific applications and in many applications and devices around the world and across all sectors of the global economy, as described in Report ITU-R M.2458;

c) that harmful interference to the RNSS has potential consequences for safety systems used by aeronautical and maritime applications, and for the regularity and efficiency of civil aviation operations;

d) that the International Civil Aviation Organization (ICAO) has taken action to reinforce the resilience to interference of aeronautical positioning, navigation and timing (PNT) systems (see

resolves to urge administrations

1 to apply necessary measures to avoid the proliferation, circulation and operation of unauthorized transmitters that cause, or have the potential to cause, harmful interference to RNSS systems and networks operating in the frequency bands 1 164-1 215 MHz and 1 559-1 610 MHz, including possible measures that might need to be taken with respect to *recognizing j)*;

2 to take the following actions to prevent and mitigate harmful interference affecting the RNSS operating in the frequency bands 1 164-1 215 MHz and 1 559-1 610 MHz without prejudice to the right of administrations to deny access to the RNSS, for security or defence purposes:

This explicit caveat implies that GNSS interference is here to stay: Any country claiming a defensive purpose can jam or spoof GNSS with impunity.

Mind the Distribution

THE UNIVERSITY OF TEXAS AT AUSTIN
RADIONAVIGATION LABORATORY

The interplay between attacker and defender in EW is best understood in terms of signal orthogonality and probability theory.

Frequency

f

Time

t

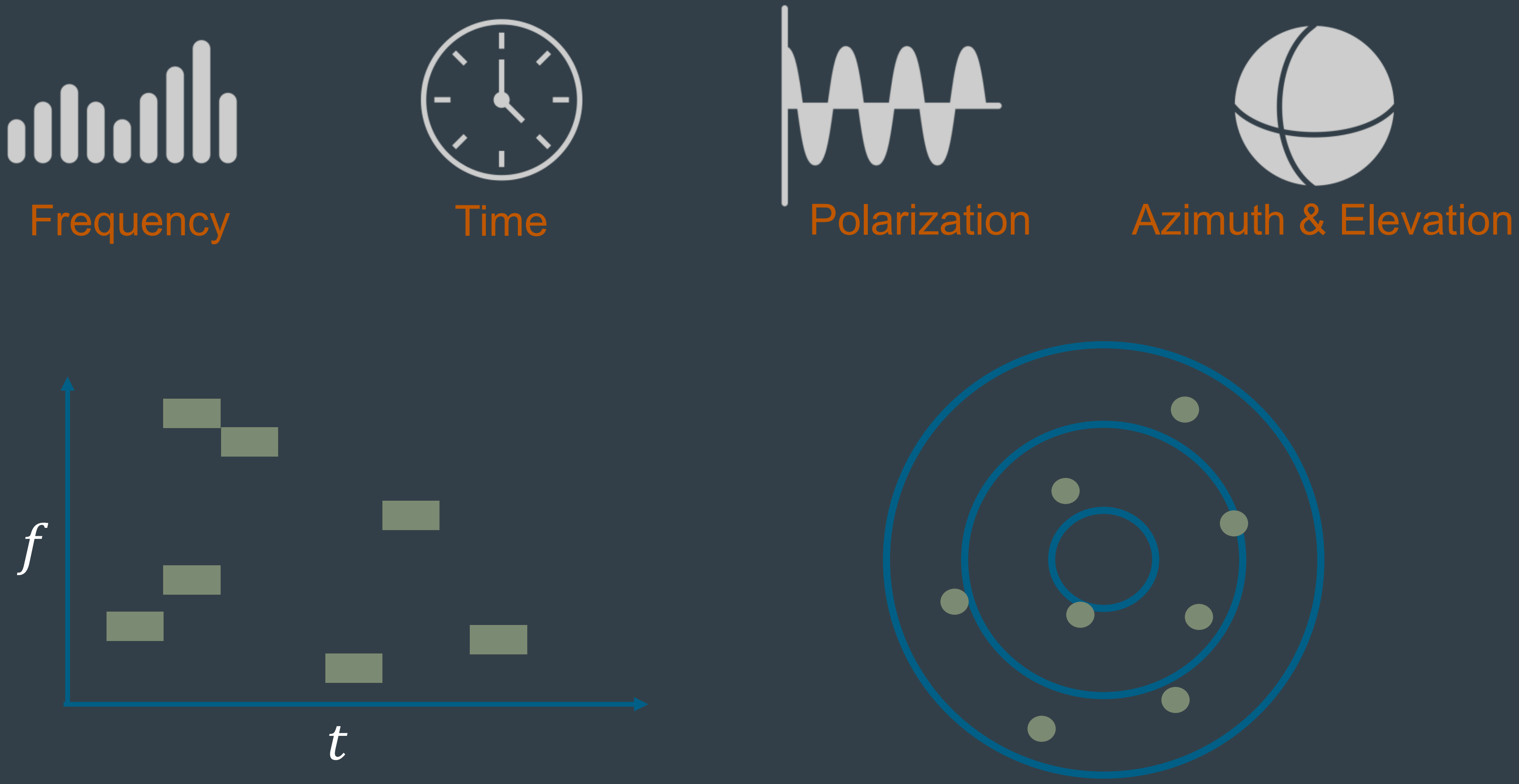
Polarization

β

Azimuth & Elevation

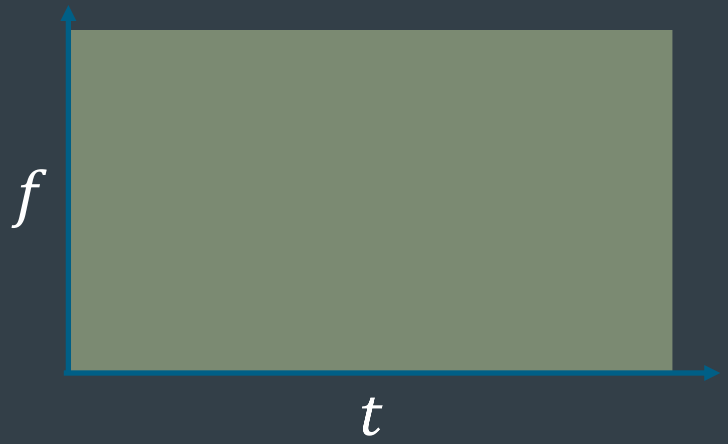
θ, ϕ

The practical EW parameter space is 5-dimensional. Two received signals are *orthogonal* if they are sufficiently different from each other along any one of these dimensions.

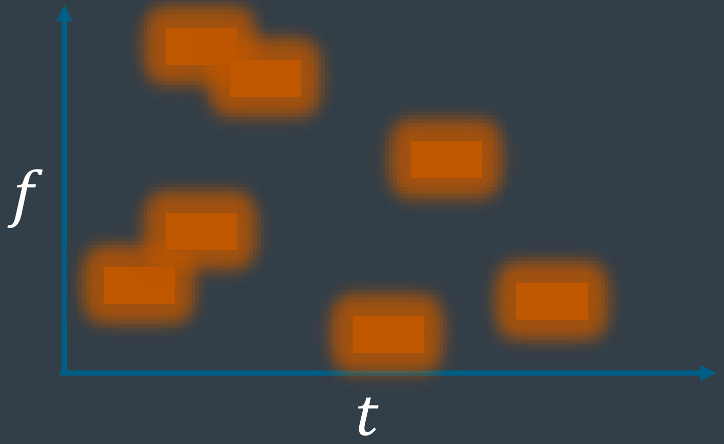


Defender's goal: Maintain all vital links above SNR thresholds

Frequency Time Polarization Azimuth & Elevation

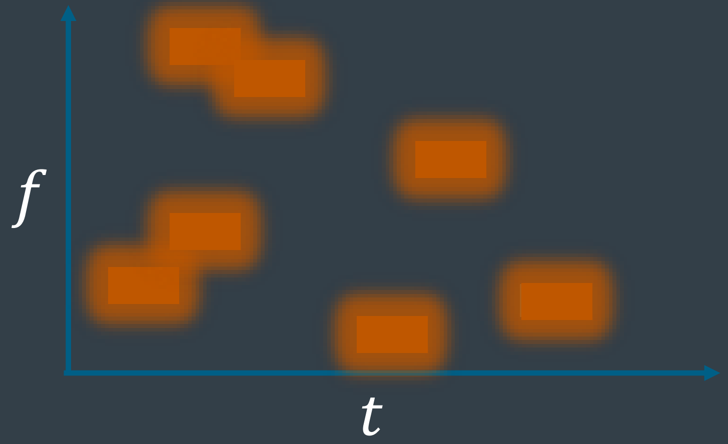


Defender's strategy: Force attacker to assume a *diffuse prior* across all dimensions so that interference signals will likely be *orthogonal* to desired signals.



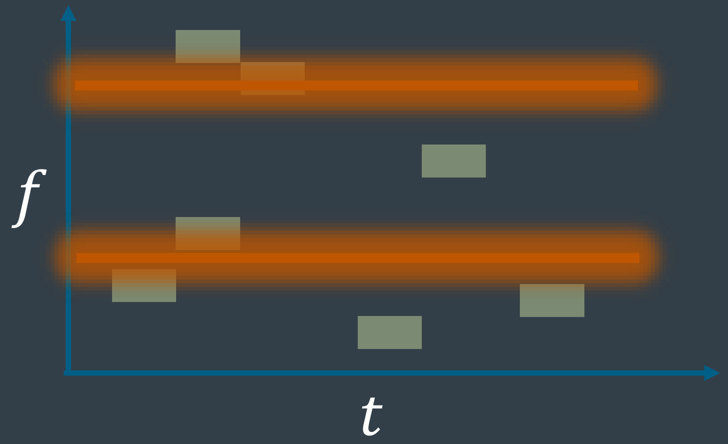
Jammer’s goal: Deny defender’s vital links as inconspicuously as possible

Frequency | Time | Polarization | Azimuth & Elevation



Jammer's strategy: Efficiently eclipse authentic signals; maximize *overlap*

Frequency | Time | Polarization | Azimuth & Elevation



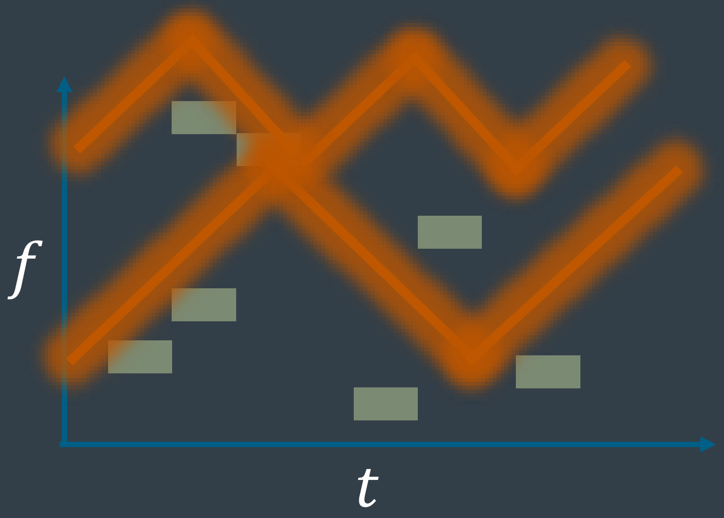
Naïve jamming: Conspicuous and ineffectual

Frequency

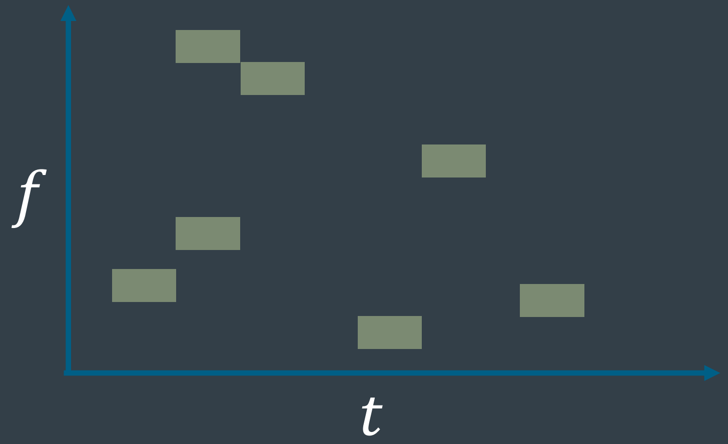
Time

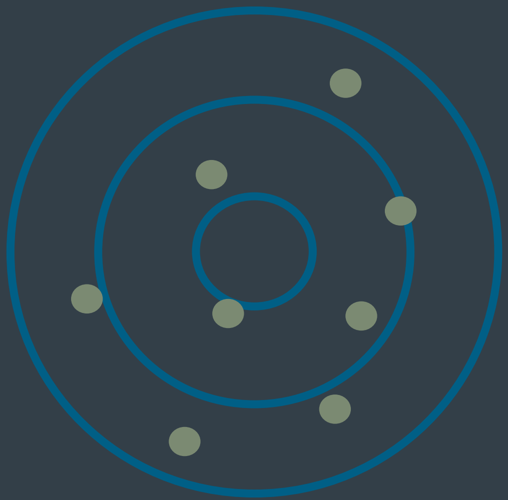
Polarization

Azimuth & Elevation

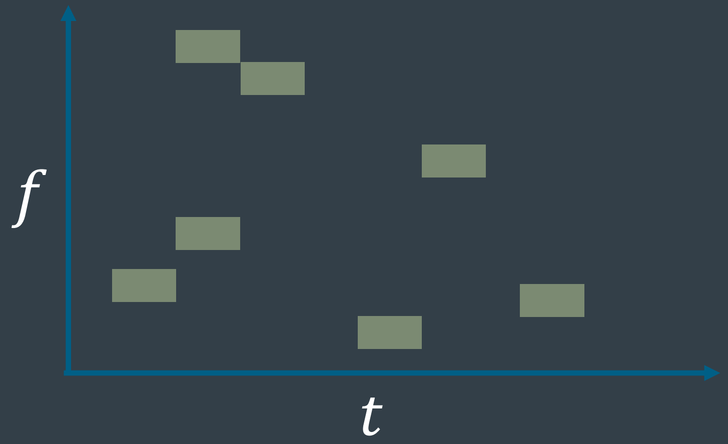


Naïve jamming: Conspicuous and ineffectual





Spoofer’s goal: Deceive or deny vital links



Spoofer's strategy: Mimic authentic signals across parameter space and (if possible) content

Green field PNT

THE UNIVERSITY OF TEXAS AT AUSTIN
RADIONAVIGATION LABORATORY

Q: If one were to design a wholly new radio-based PNT system with the benefit of hindsight, how would it look?

Frequency

f

Time

t

Polarization

β

Azimuth & Elevation

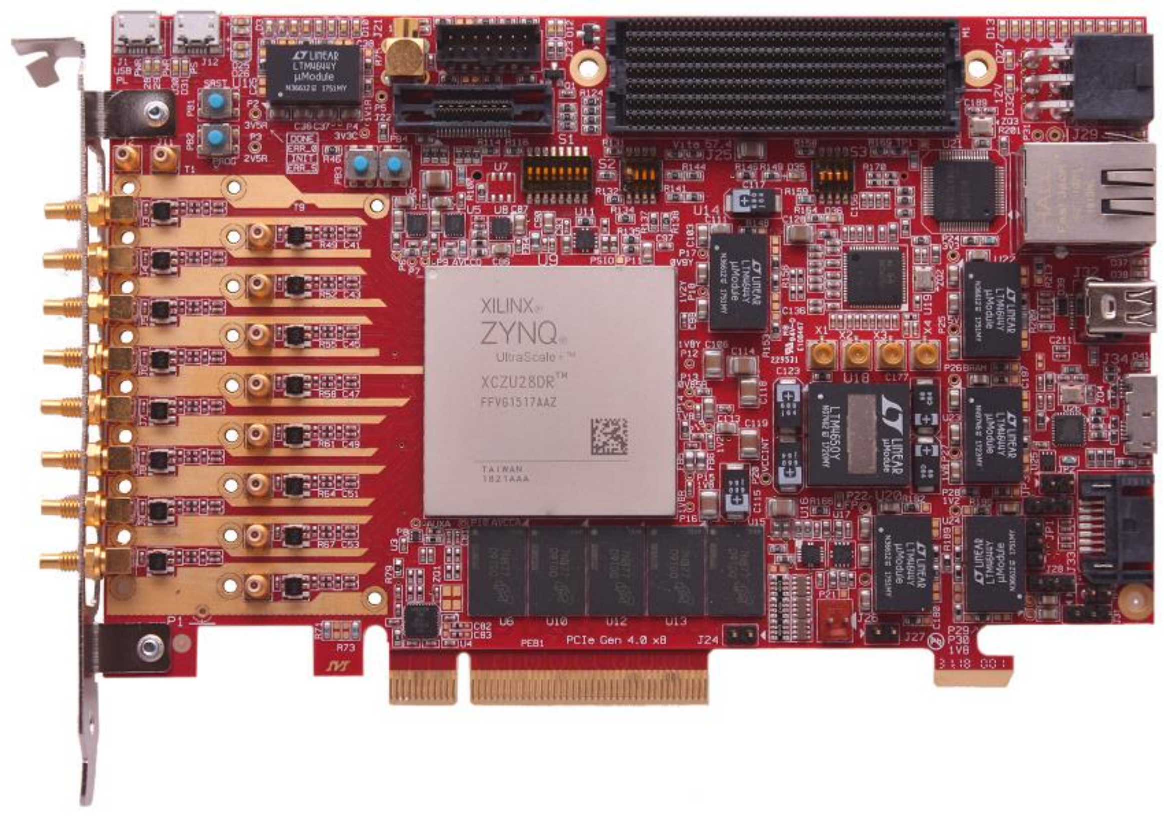
θ, ϕ

Inexpensive flexibility within the 5-D parameter space

Time

Frequency

Primary benefit is extraordinary time/frequency agility



Xilinx RFSOC: 8 ADC/DAC ports. 12-bit ADCs @ 4.1 Gsps. Powerful FPGA with embedded CPU. All for less than 40 dB$.

Azimuth & Elevation

Polarization

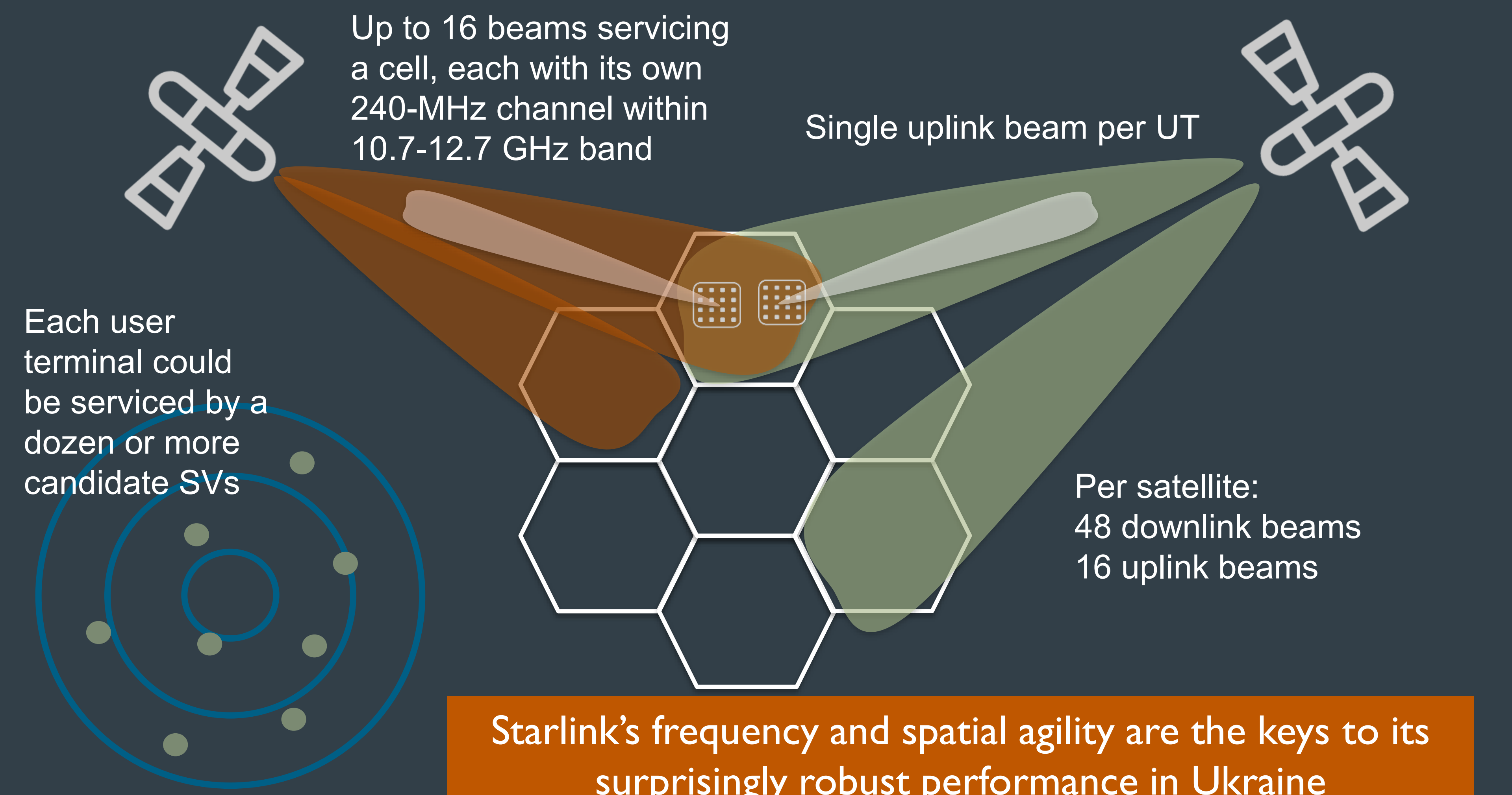
Extraordinary spatial and polarization agility

2019 $3k

2021 $1.3k

2024 $600

Starlink user terminal epitomizes recent advances in phased array technology.
Half duplex, single-beam 30-35 dBi gain (6.4-3.6 deg. beamwidth).



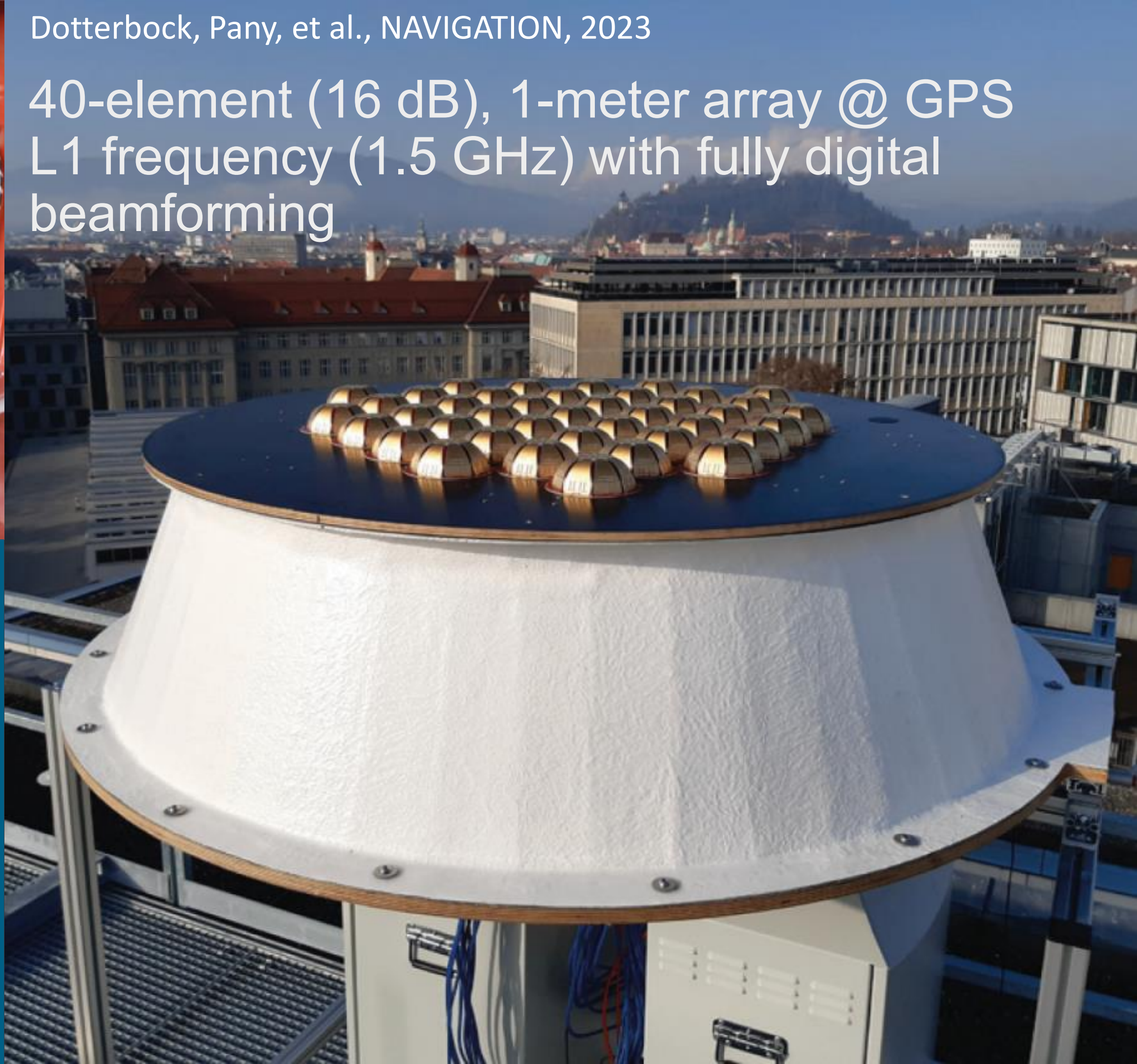
Starlink's frequency and spatial agility are the keys to its surprisingly robust performance in Ukraine

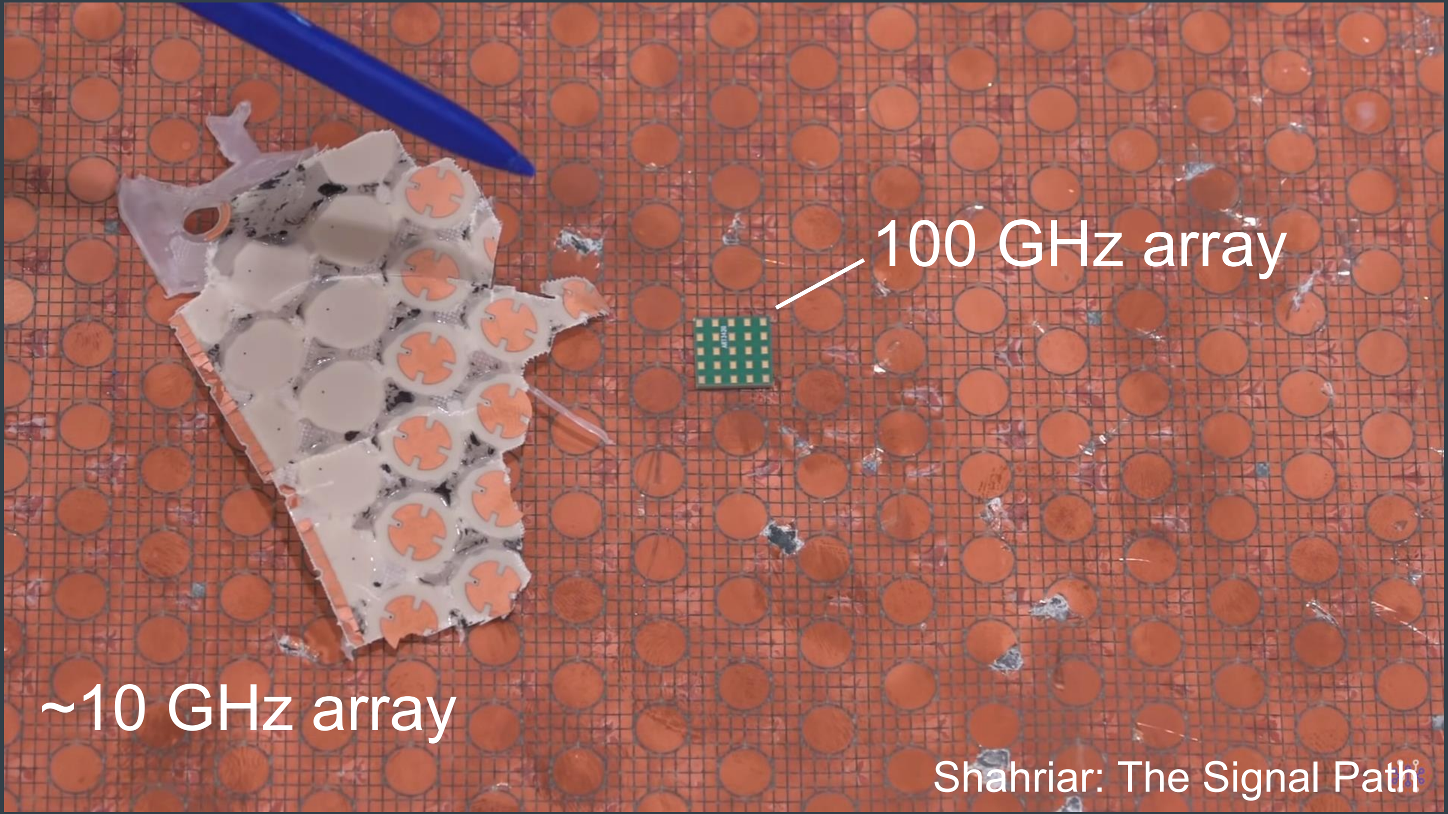
(1) Beamforming is more cumbersome at lower frequencies (e.g., L-band).

(2) Fully digital beamforming is highly flexible but expensive *and susceptible to amplifier/ADC saturation in hostile RF environments.*

Dotterbock, Pany, et al., NAVIGATION, 2023

40-element (16 dB), 1-meter array @ GPS L1 frequency (1.5 GHz) with fully digital beamforming

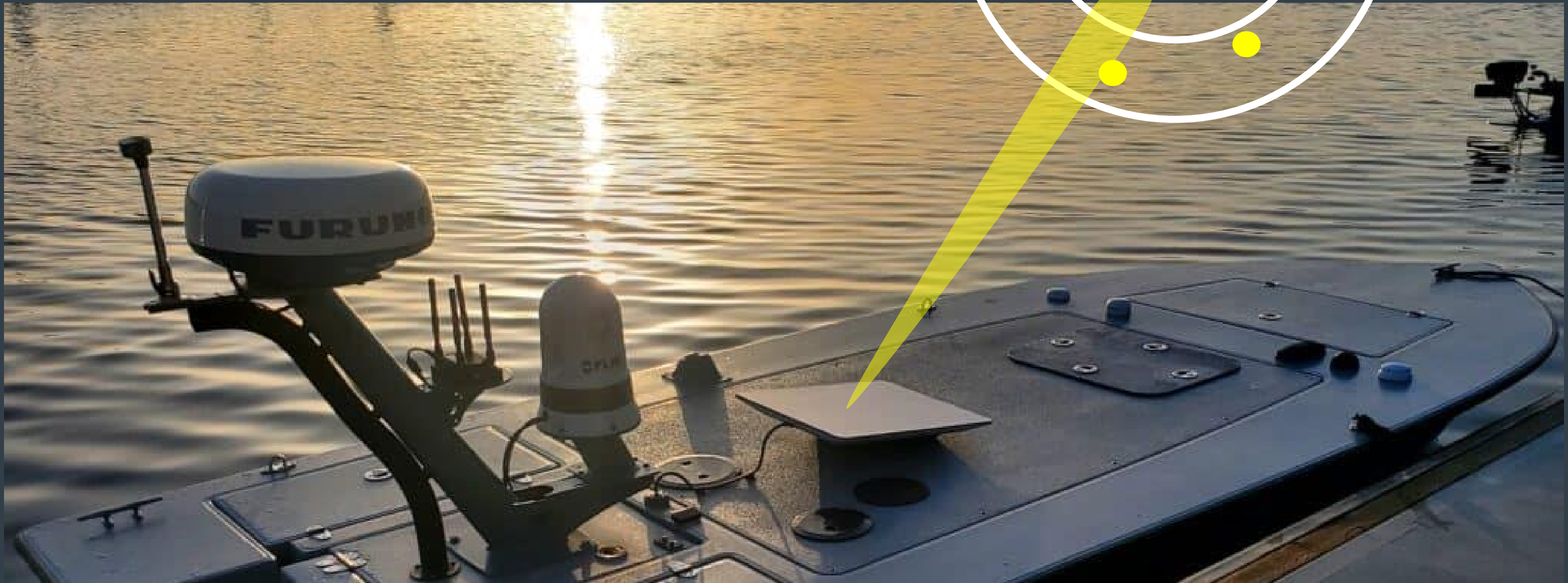


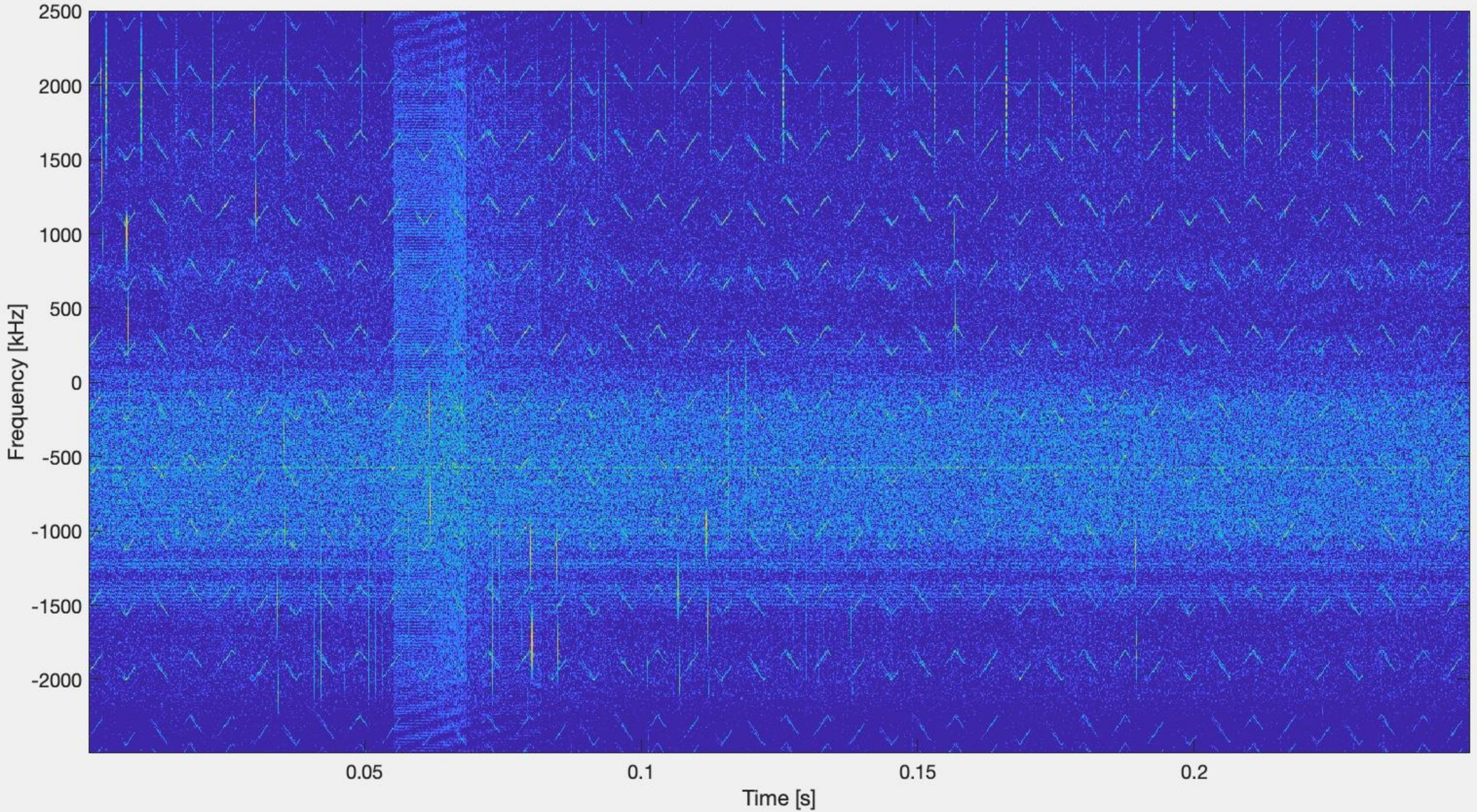


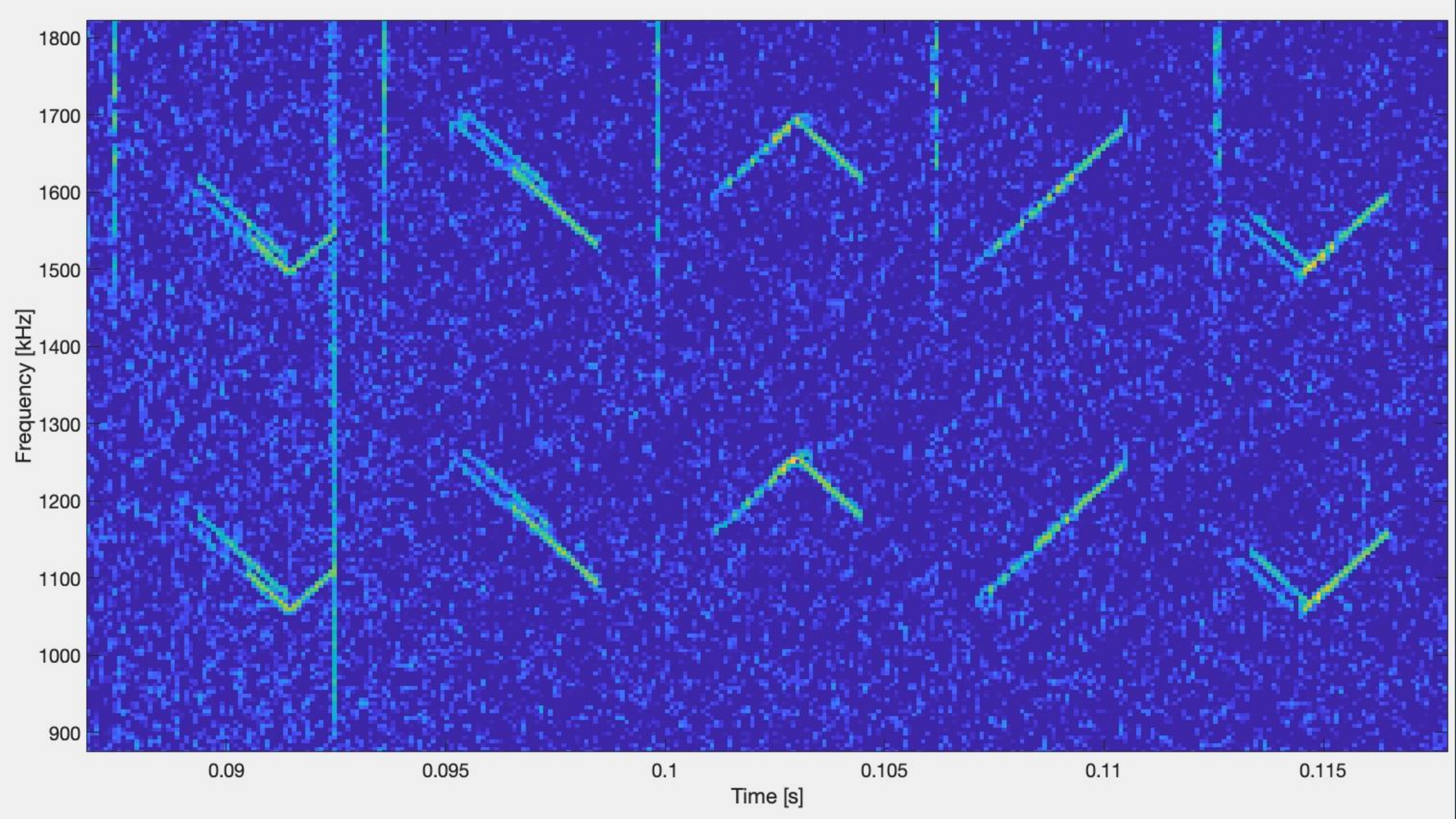
Higher frequencies beckon: "Tightbeam" point-to-point comms possible with compact arrays; e.g., 10-cm-diameter 36-dB (3-deg-beam) arrays @ 100 GHz. Can costs be made competitive with Starlink user terminal?

Space deployment allows for enormous arrays even at sub-GHz frequencies. Bluewalker 3 satellite focuses dozens of ~ 2.5-deg. beams on surface to support direct-to-handset comms.

Tight beams oriented in unpredictable directions pose a daunting challenge for offensive EW.

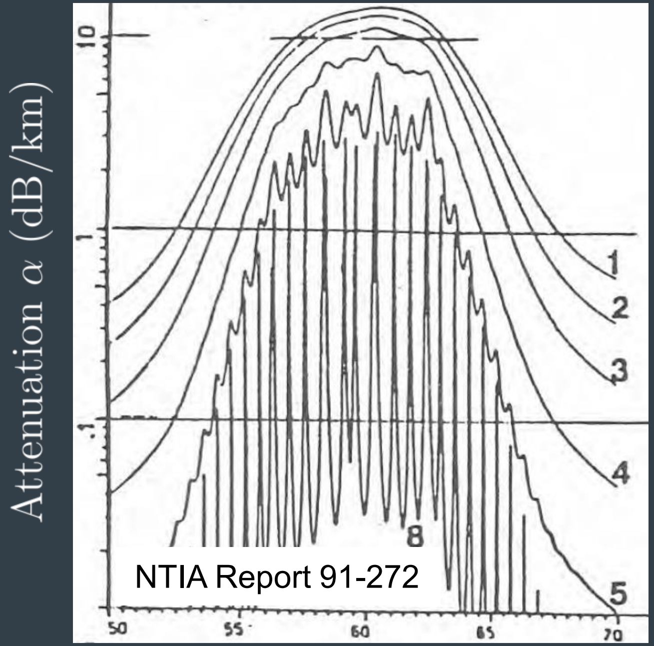



2500
2000
1500
1000
500
0
-500
-1000
-1500
-2000
Frequency [kHz]
0.05
0.1
0.15
0.2
Time [s]



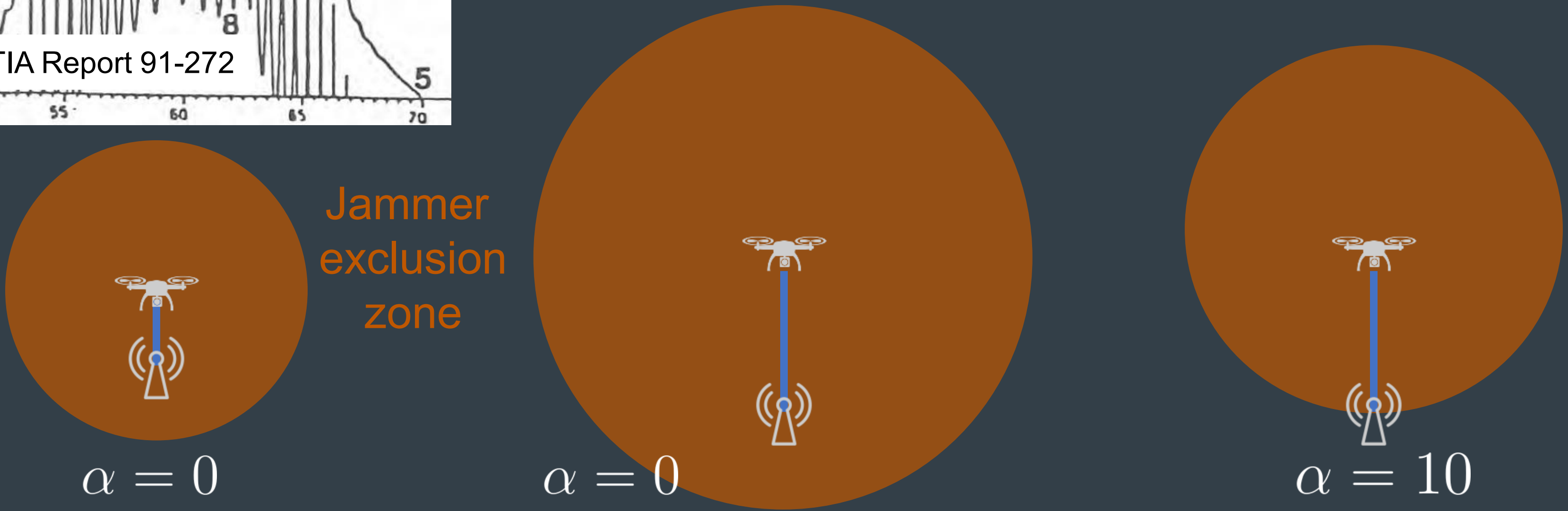
Frequency [kHz]
1800
1700
1600
1500
1400
1300
1200
1100
1000
900
0.09
0.095
0.1
0.105
0.11
0.115
Time [s]

As a last resort, a defender can hide behind the O_2 line.



$$\frac{J}{S} = \left(\frac{J}{S}\right)_0 + 20\log_{10}\left(\frac{r_T}{r_I}\right) + \alpha\left(r_T - r_I\right)$$

A simple rule for hiding behind the O_2 line: The nearest transmitter dominates.



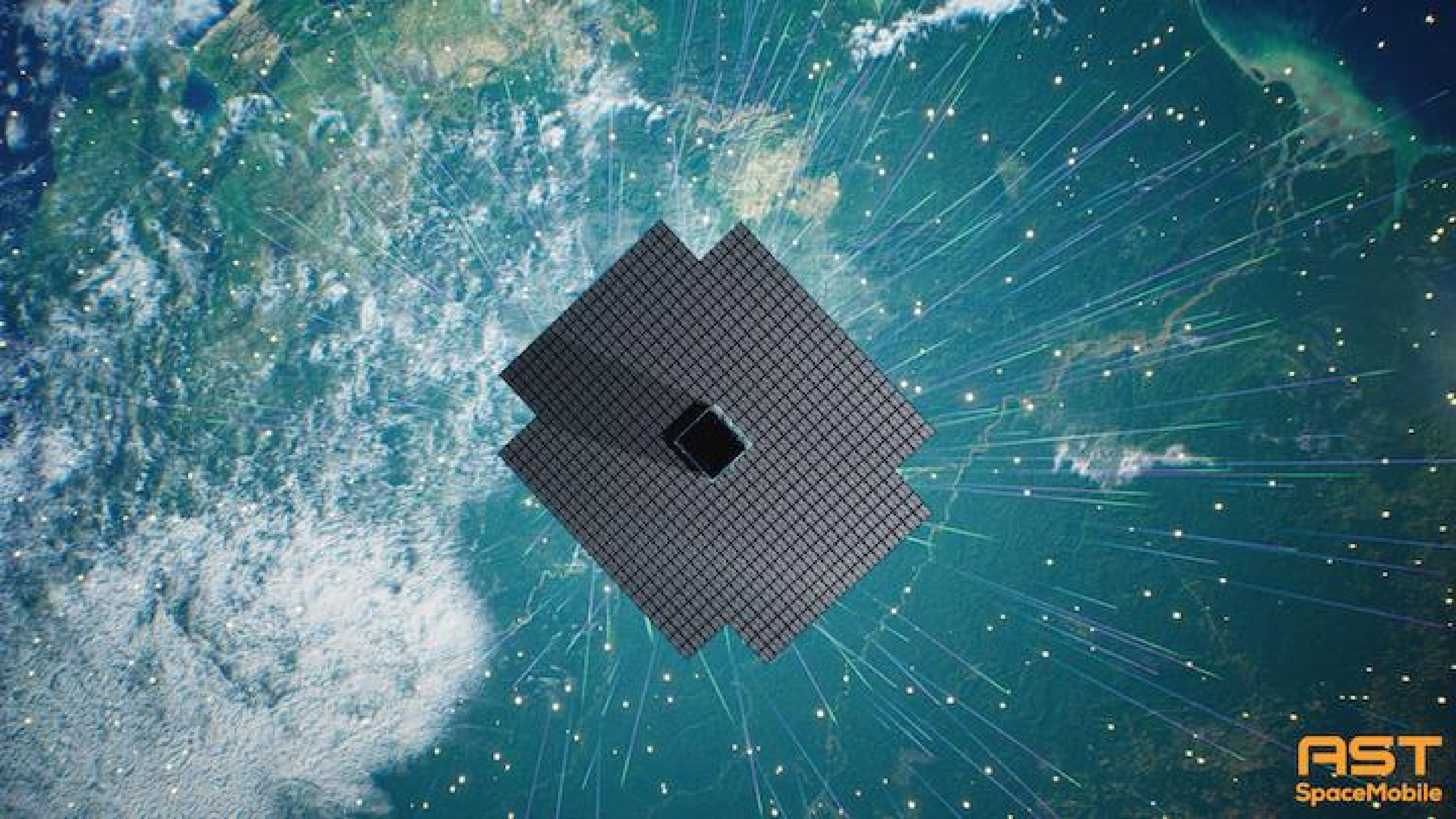
Escalation

THE UNIVERSITY OF TEXAS AT AUSTIN
RADIONAVIGATION LABORATORY

The tables being tilted in favor of defense may eventually provoke a radical response.

~100 kW nuclear power unit

Russia may be pursuing a radical escalation of EW:
A nuclear-powered interference source in space. Project Ekipazh.


AST
SpaceMobile

THE UNIVERSITY OF TEXAS AT AUSTIN
RADIONAVIGATION LABORATORY