THE UNIVERSITY OF TEXAS AT AUSTIN
RADIONAVIGATION LABORATORY

GNSS Radio Frequency Interference Detection from Low Earth Orbit

Matthew J. Murrian, Lakshay Narula, Peter Iannucci, and Todd E. Humphreys

Department of Aerospace Engineering and Engineering Mechanics

The University of Texas at Austin

INC 2019, Edinburgh | November 19, 2019


Black Sea: 2016-2019


Northern Norway: October 2018


Syria: 2018-2019
Ben Gurion Airport: March-July, 2019


Port of Shanghai: Oct. 2018 -- Aug. 2019

A flexible, science-grade GNSS receiver in low-earth orbit (LEO) would enable continuous global monitoring and characterization of GNSS interference

Q: What interference EIRP could be detected?

Q: What would be the rate of detection?

Q: How accurately could source be geolocated?

Detection

$$\mathrm{CINR} \triangleq \frac{C}{N_0 + I_0}$$

C/N0 Observable under Interference

$$H_0 : \boldsymbol{z} \sim \mathcal{N}(\boldsymbol{\mu}, P)$$
$$H_1 : \boldsymbol{z} \sim \mathcal{N}(\boldsymbol{\mu} - \delta \mathbf{1}, P)$$

Hypothesis Test

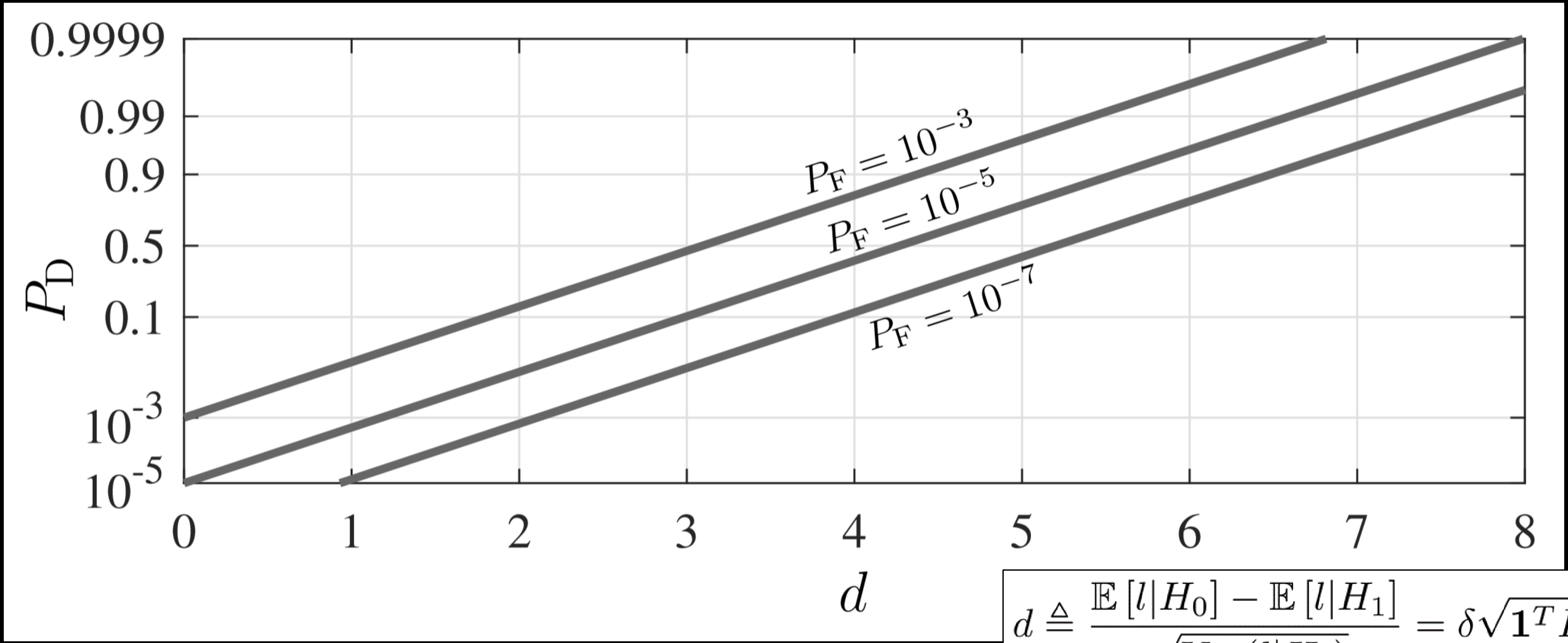
$$l(\boldsymbol{z}) = \mathbf{1}^T P^{-1} \boldsymbol{z} \underset{H_1}{\overset{H_0}{\gtrless}} \nu$$

Likelihood Ratio Test

A hypothesis test for interference can be formulated in terms of a common decrease in CINR measurements due to an increase in I_o.

Received Power could also be used in place of **CINR**: no tracking required.

Detection



$$d \triangleq \frac{\mathbb{E}\left[l|H_0\right] - \mathbb{E}\left[l|H_1\right]}{\sqrt{\mathrm{Var}(l|H_0)}} = \delta\sqrt{\mathbf{1}^T P^{-1}\mathbf{1}}$$

Performance of the interference detection test is completely characterized by the normalized distance between the means of the detection statistic $l(\mathbf{z})$ under H_0 and H_1.

Detection Sensitivity

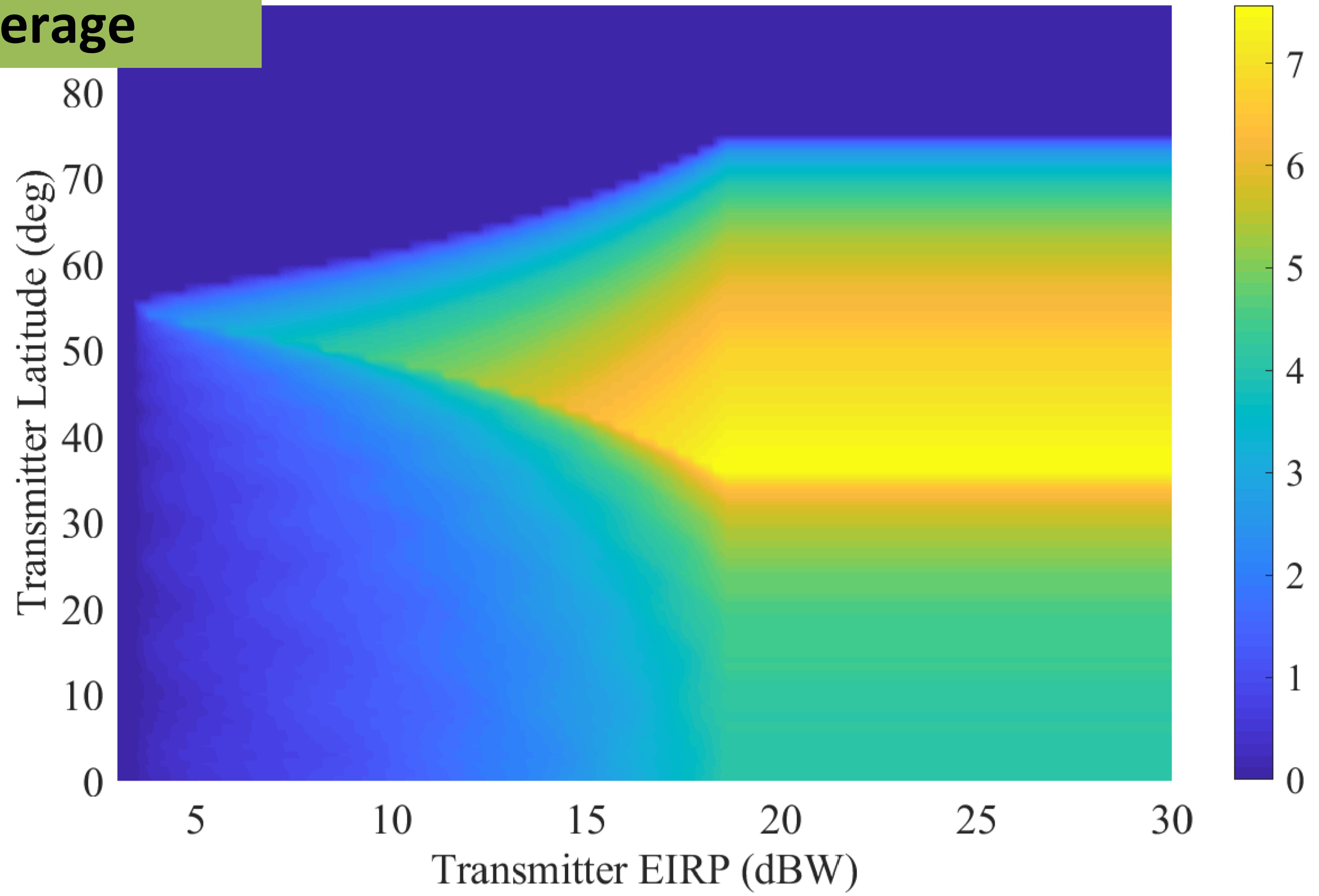
Detection Method	Minimum Detectable EIRP
C/N0	3.5 dBW
Received Power	3.5 dBW
Signal Acquisition	-28.5 dBW

Assumptions:

- $P_F = 10^{-5}, \quad P_D > 0.9$
- 4-MHz BW uniform interference at L1
- 3 dB receiver antenna gain, 400 km satellite altitude, transmitter at sea level
- 30 dB-Hz acquisition threshold for signal acquisition.

Matched-code interference can be detected with high-sensitivity by signal acquisition

Coverage



Average number of transmitter detections per day by a monitoring satellite on an ISS-like orbit.

Coverage

Worst-case time between detections:
6.1 dBW EIRP: 4 days
3.7 dBW EIRP: 17 days

Assumptions:

- Space-station-like orbit: 400 km, 55-deg inclination
- Transmitter at sea level

Geolocation Accuracy

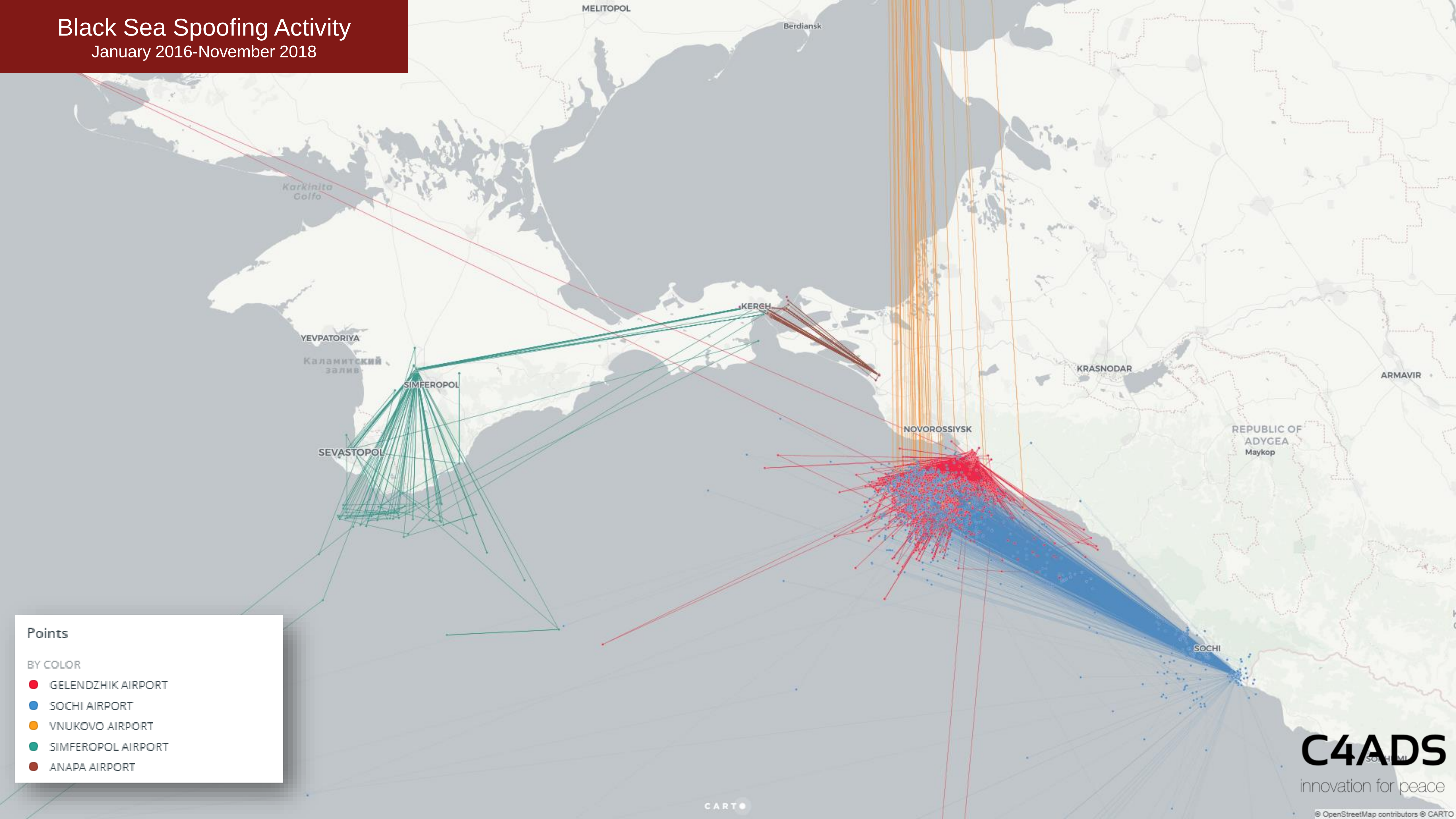
Dual satellites (joint FDOA-TDOA): ~1 km CEP

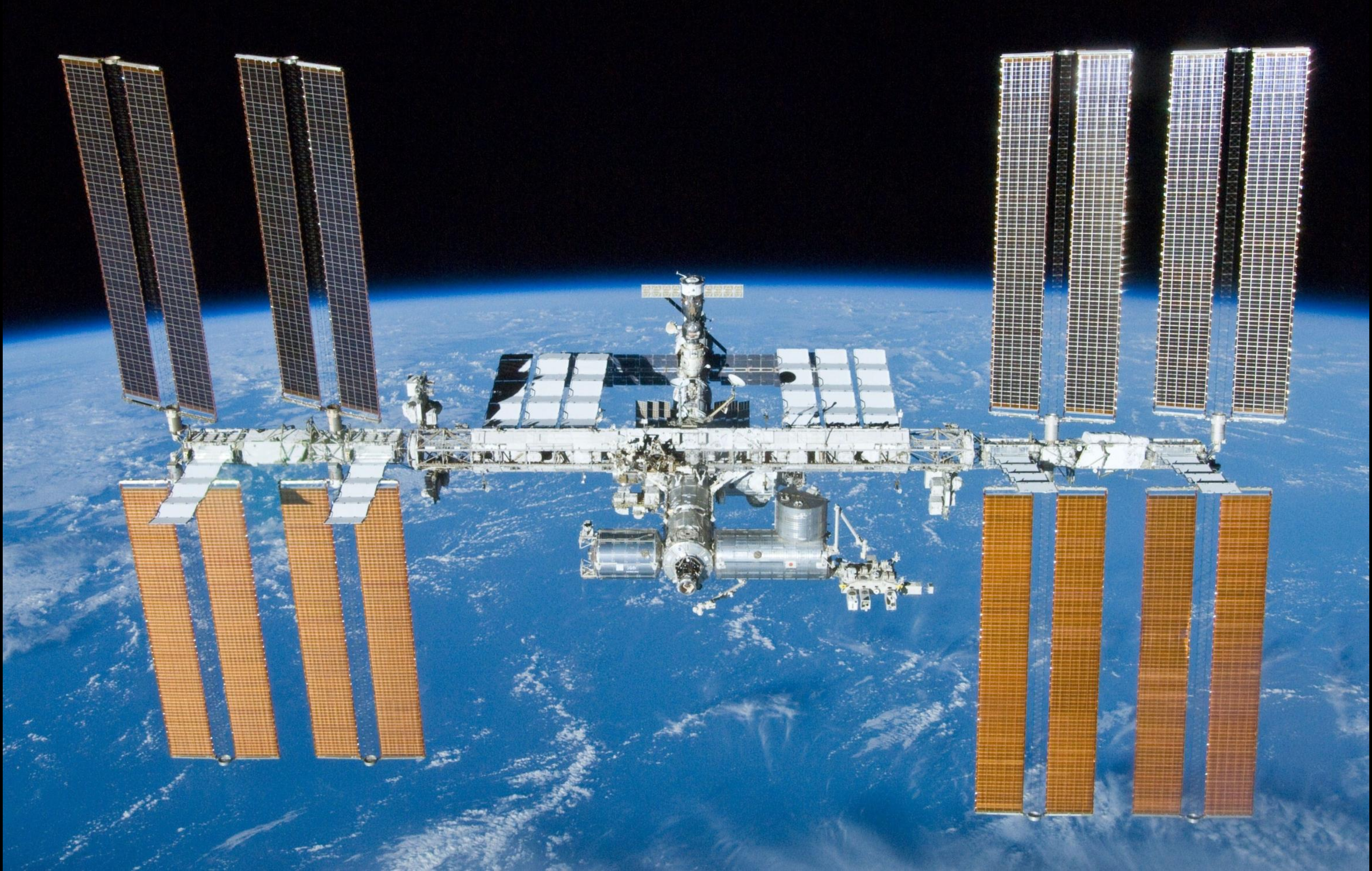
Single satellite (Doppler positioning): ~3 km CEP

Assumptions:

- Space-station-like orbit: 400 km, 55-deg inclination
- 50-km inter-satellite baseline (for dual satellite scenario)
- Transmitter at sea level
- 100-W EIRP transmitter with low-quality OCXO
- Single flyover

Black Sea Spoofing Activity
January 2016-November 2018





February 2017: FOTON SDR installed on International Space Station

Science mission: Ionospheric sensing via radio occultation and airglow meas.

Collaborators: Naval Research Lab, Cornell, University of Texas, Aerospace Corp.

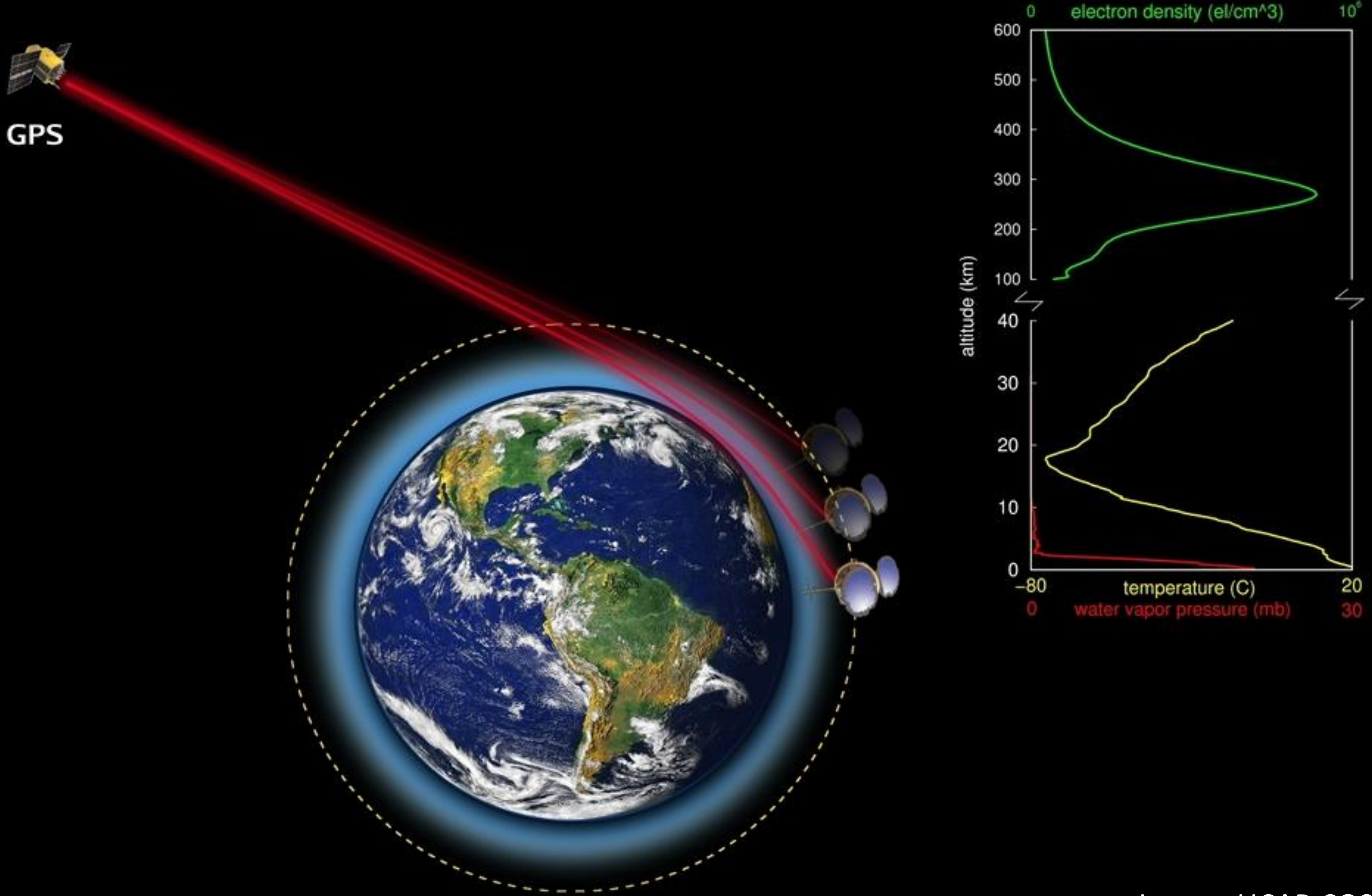
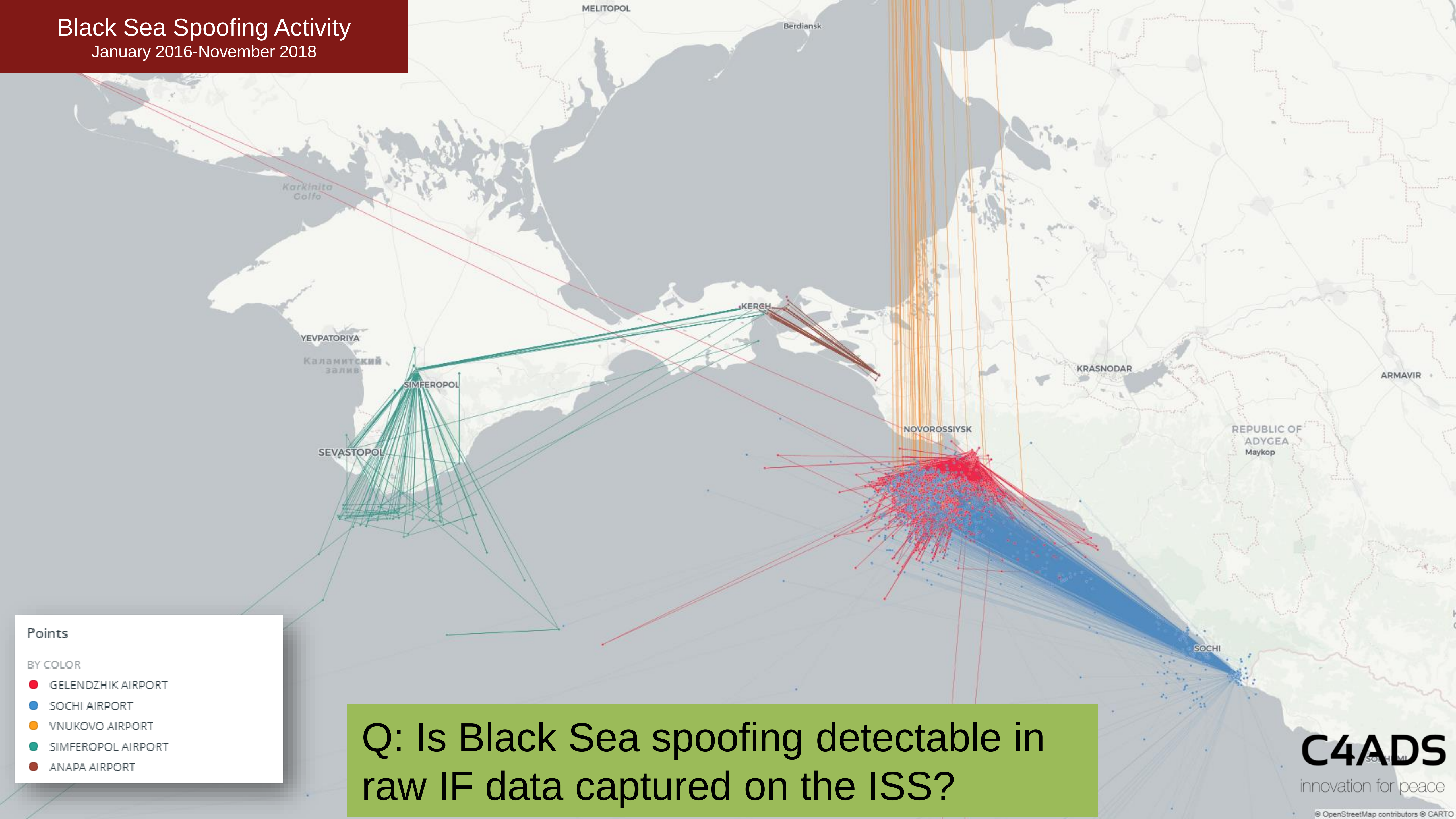


Image: UCAR COSMIC Program

Black Sea Spoofing Activity
January 2016-November 2018



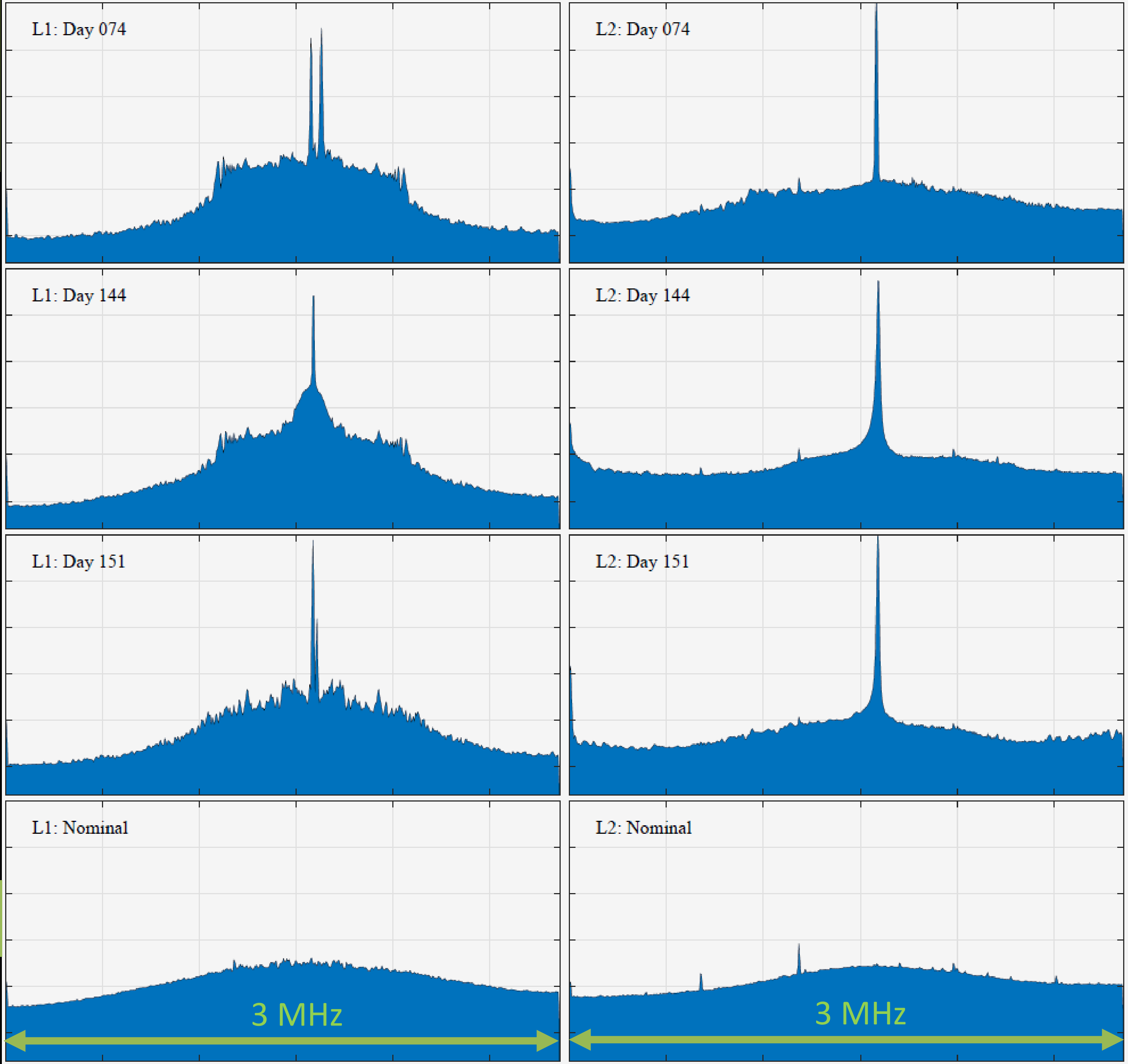
Q: Is Black Sea spoofing detectable in raw IF data captured on the ISS?

C4ADS
innovation for peace

March-May 2018: Raw IF samples captured near Black Sea on 3 separate days

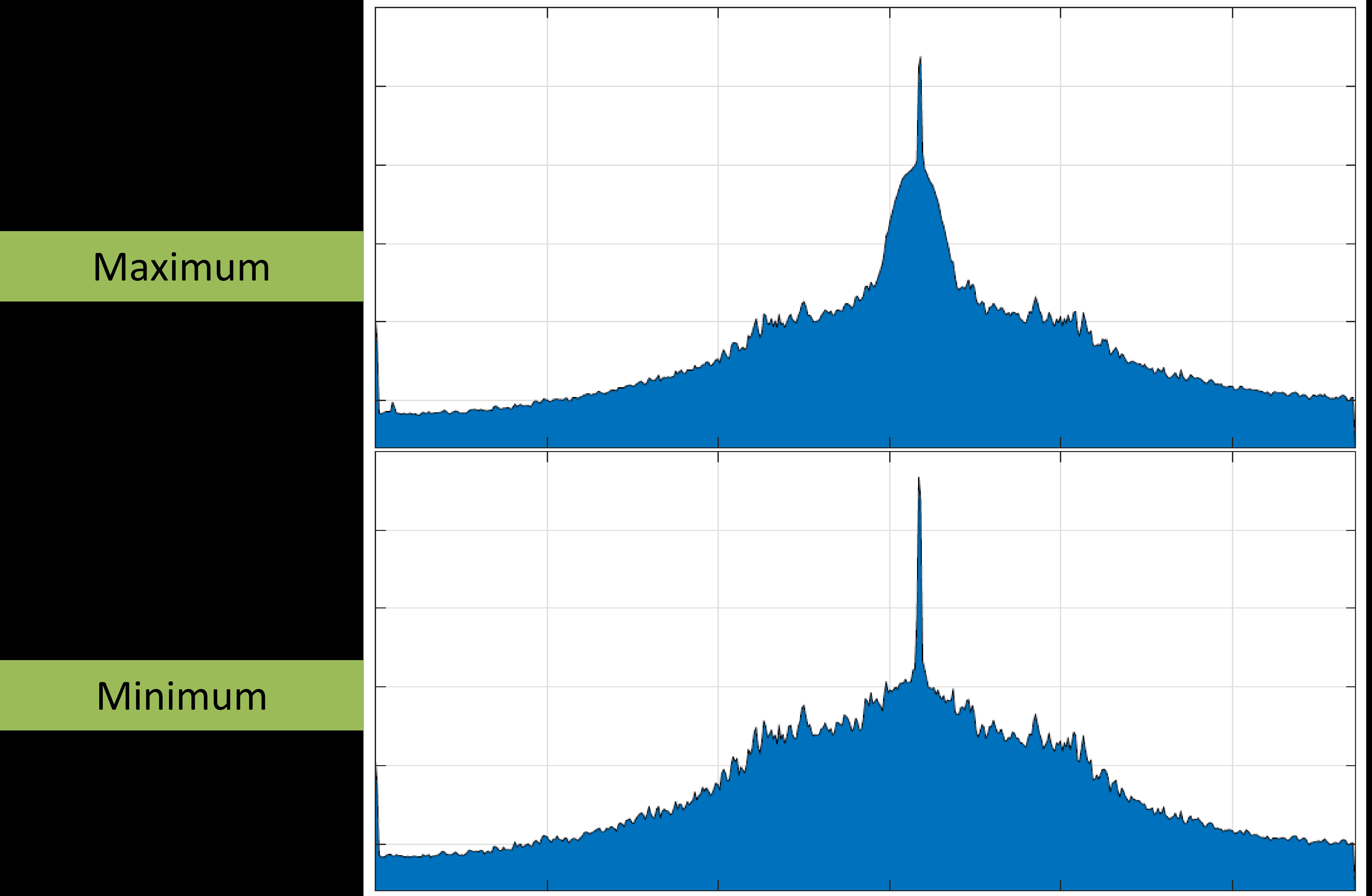
60-second recordings sent via NASA's communications backbone to NRL and thence to UT for processing with latest version of GRID

Power Spectra

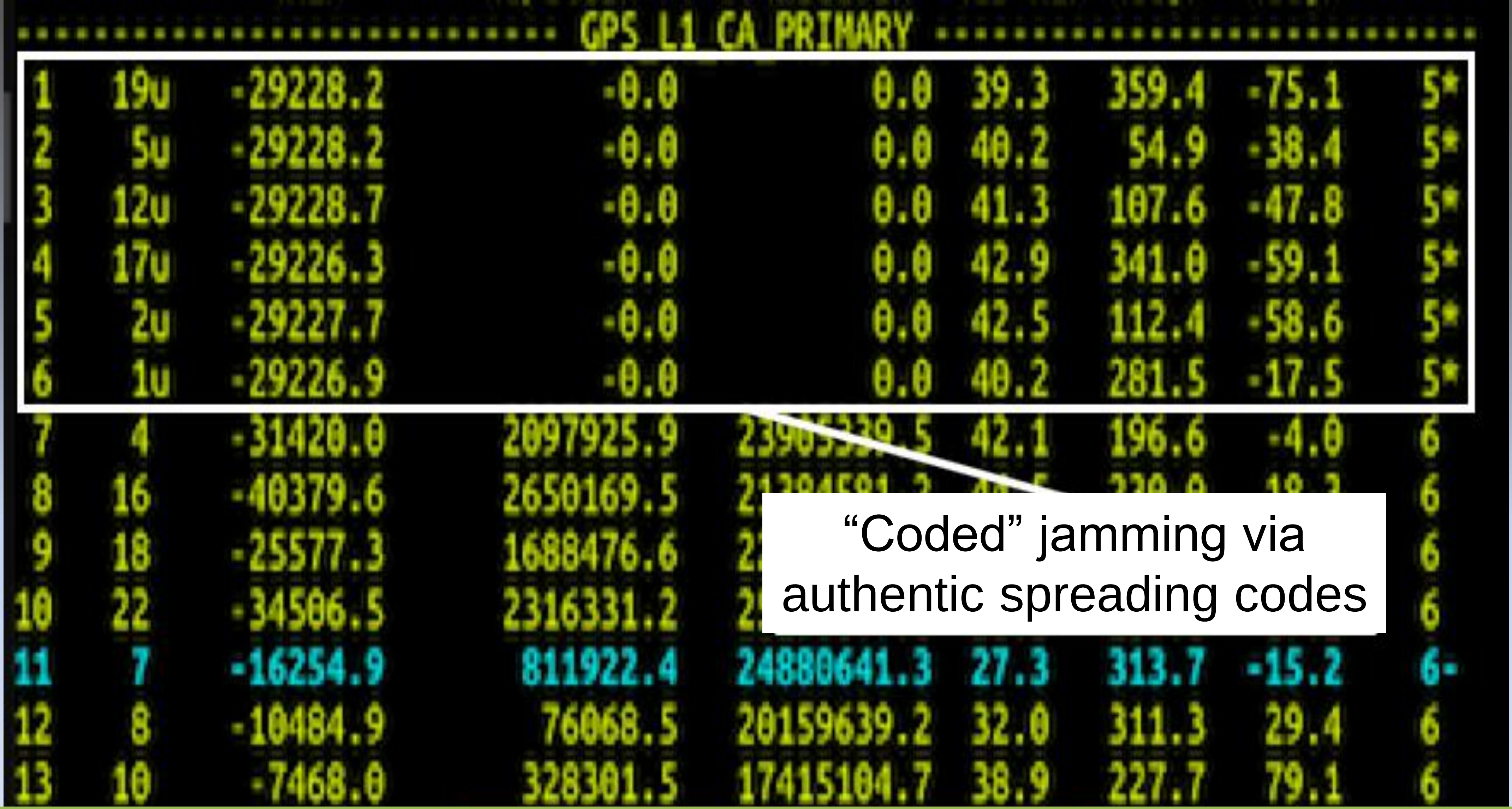


L1: 1575.42 MHz

L2: 1227.6 MHz



250 kHz rounded prominence at L1 waxes and wanes with an approximately 5 sec. period



1	19u	-29228.2	-0.0	0.0	39.3	359.4	-75.1	5*
2	5u	-29228.2	-0.0	0.0	40.2	54.9	-38.4	5*
3	12u	-29228.7	-0.0	0.0	41.3	107.6	-47.8	5*
4	17u	-29226.3	-0.0	0.0	42.9	341.0	-59.1	5*
5	2u	-29227.7	-0.0	0.0	42.5	112.4	-58.6	5*
6	1u	-29226.9	-0.0	0.0	40.2	281.5	-17.5	5*
7	4	-31420.0	2097925.9	[illegible]	42.1	196.6	-4.0	6
8	16	-40379.6	2650169.5	[illegible]	[illegible]	[illegible]	[illegible]	6
9	18	-25577.3	1688476.6	[illegible]	[illegible]	[illegible]	[illegible]	6
10	22	-34506.5	2316331.2	[illegible]	[illegible]	[illegible]	[illegible]	6
11	7	-16254.9	811922.4	24880641.3	27.3	313.7	-15.2	6-
12	8	-10484.9	76068.5	20159639.2	32.0	311.3	29.4	6
13	10	-7468.0	328301.5	17415104.7	38.9	227.7	79.1	6

The Syrian interference source employs *coded jamming.* Its purpose appears to be denial of GPS service, but it achieves this by *spoofing* each of the GPS L1 C/A PRN codes (albeit without LNAV modulation).

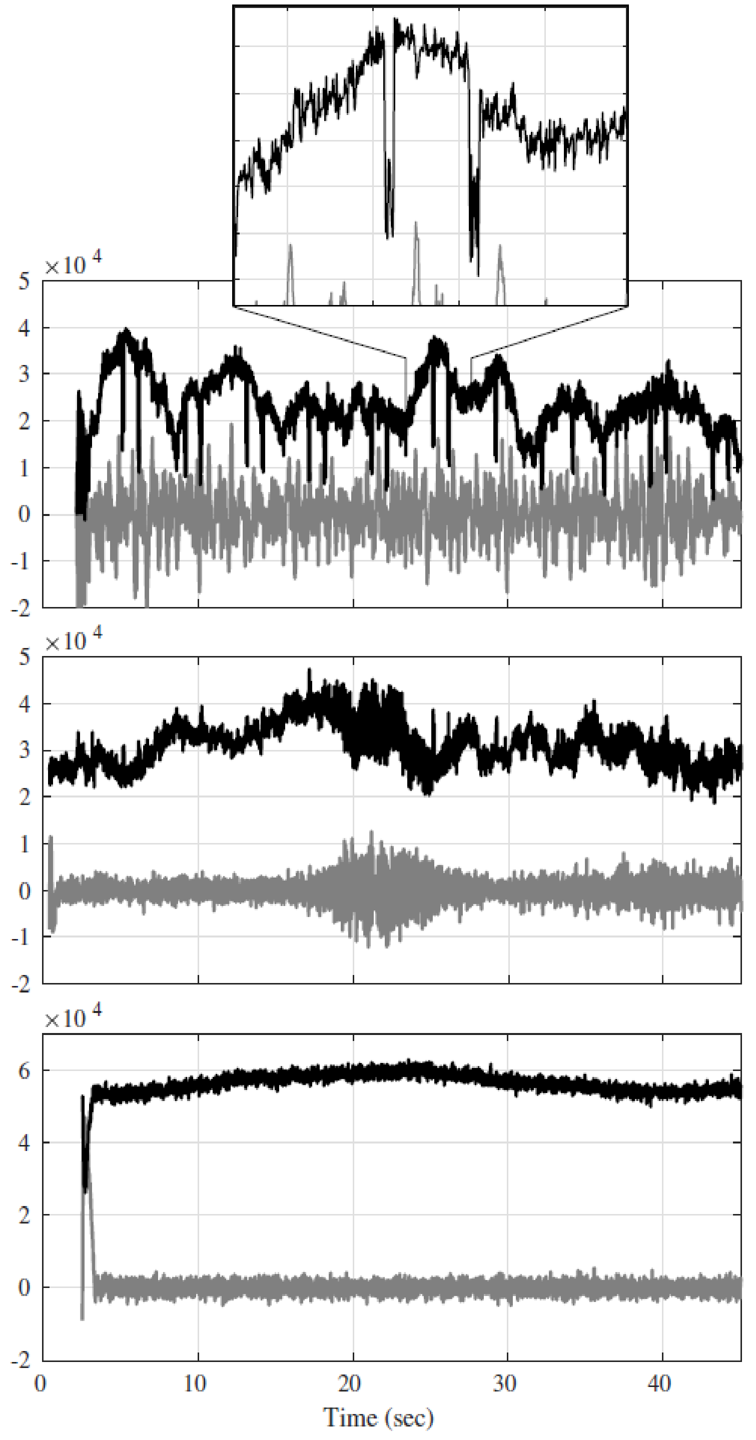
Data-Wiped 100-Hz IQ accumulations

Unexplained fading

False signal

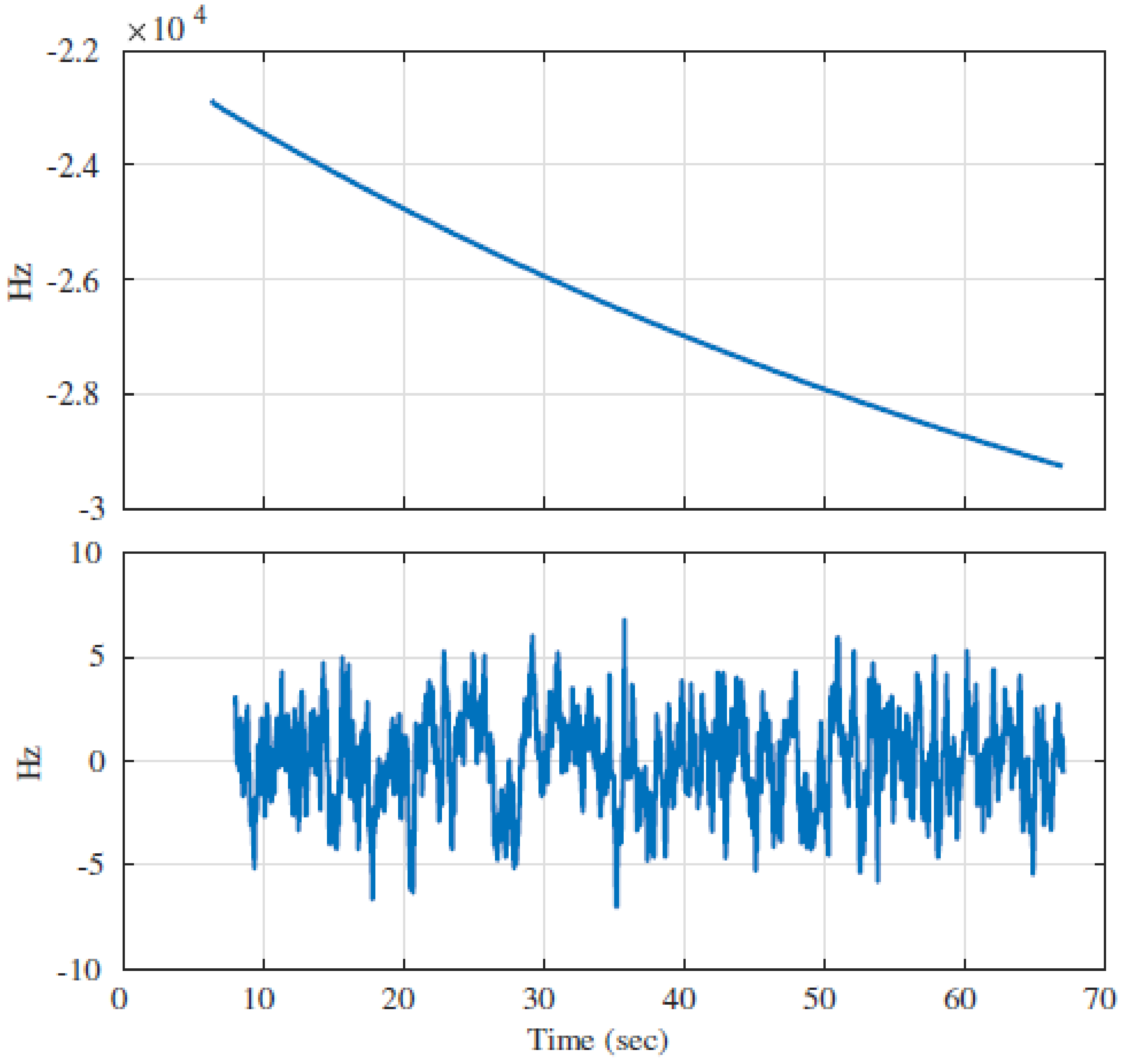
Authentic signal in interference

Authentic signal under clean conditions



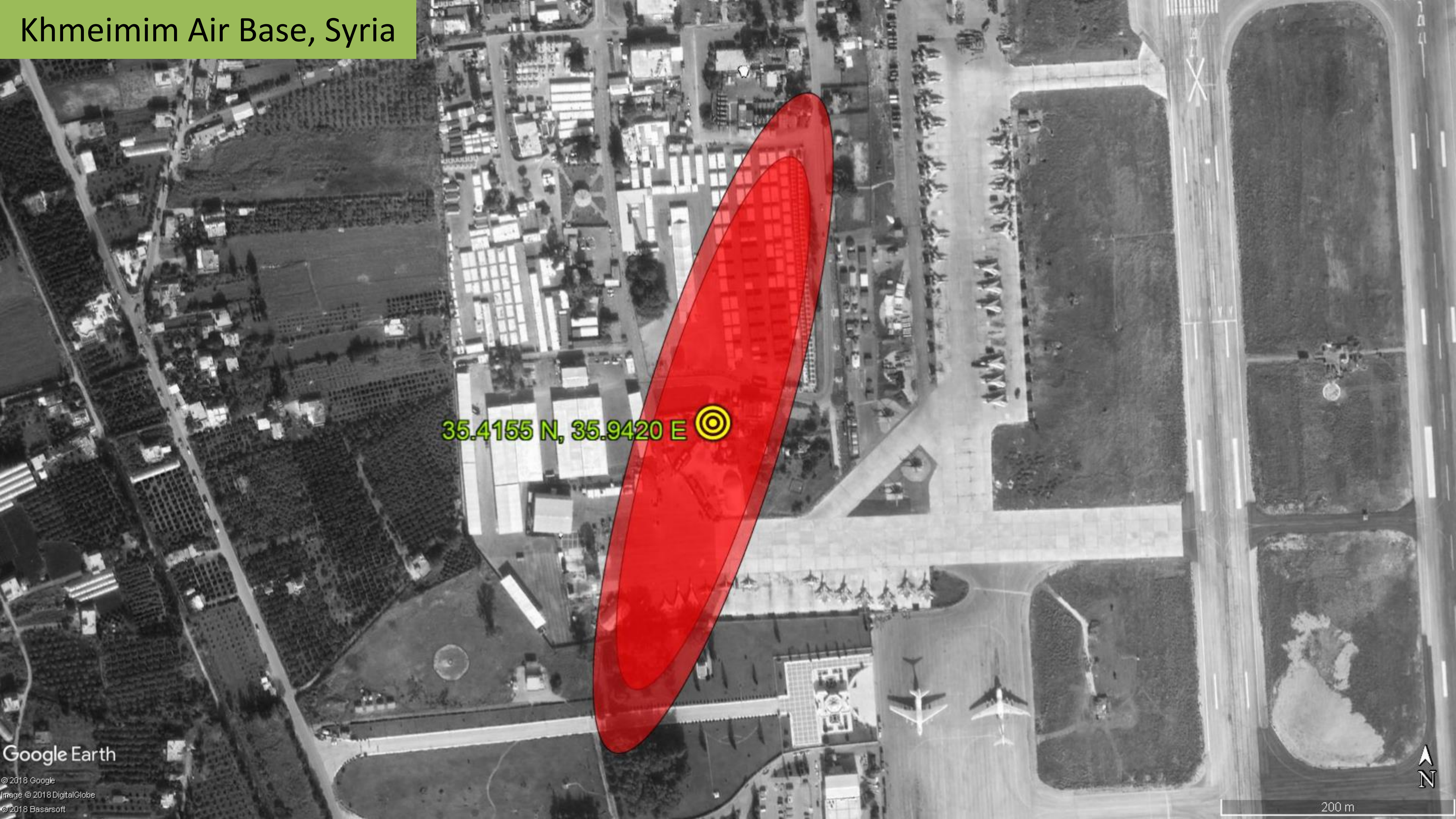
Doppler time history for false PRN 10 signal from day 144 capture

Post-fit residuals of Doppler time history assuming estimated transmitter location and clock rate offset

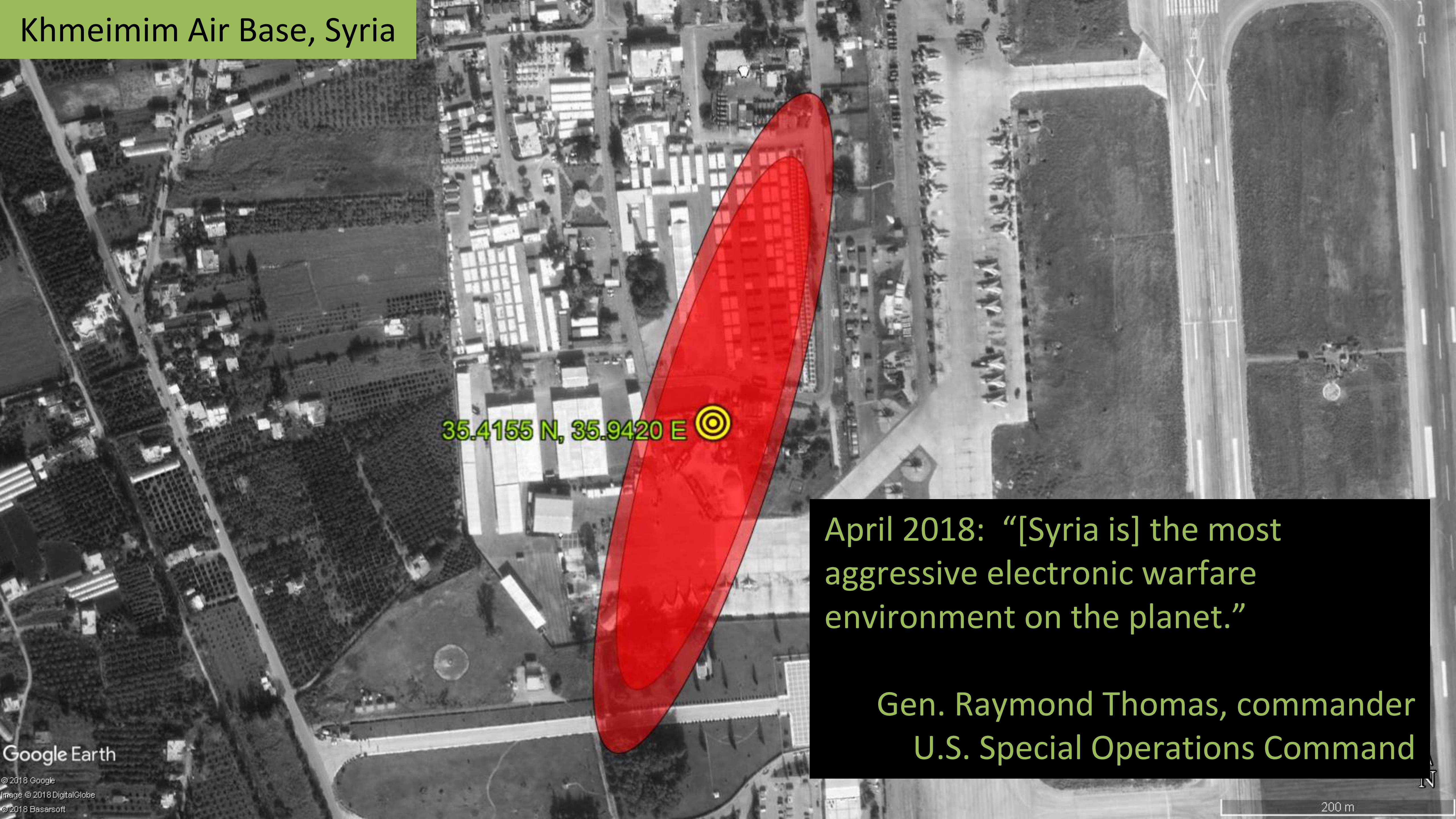


Doppler time histories can be used to infer transmitter location, assuming a transmitter clock with a constant frequency offset over each 60-second interval

Khmeimim Air Base, Syria

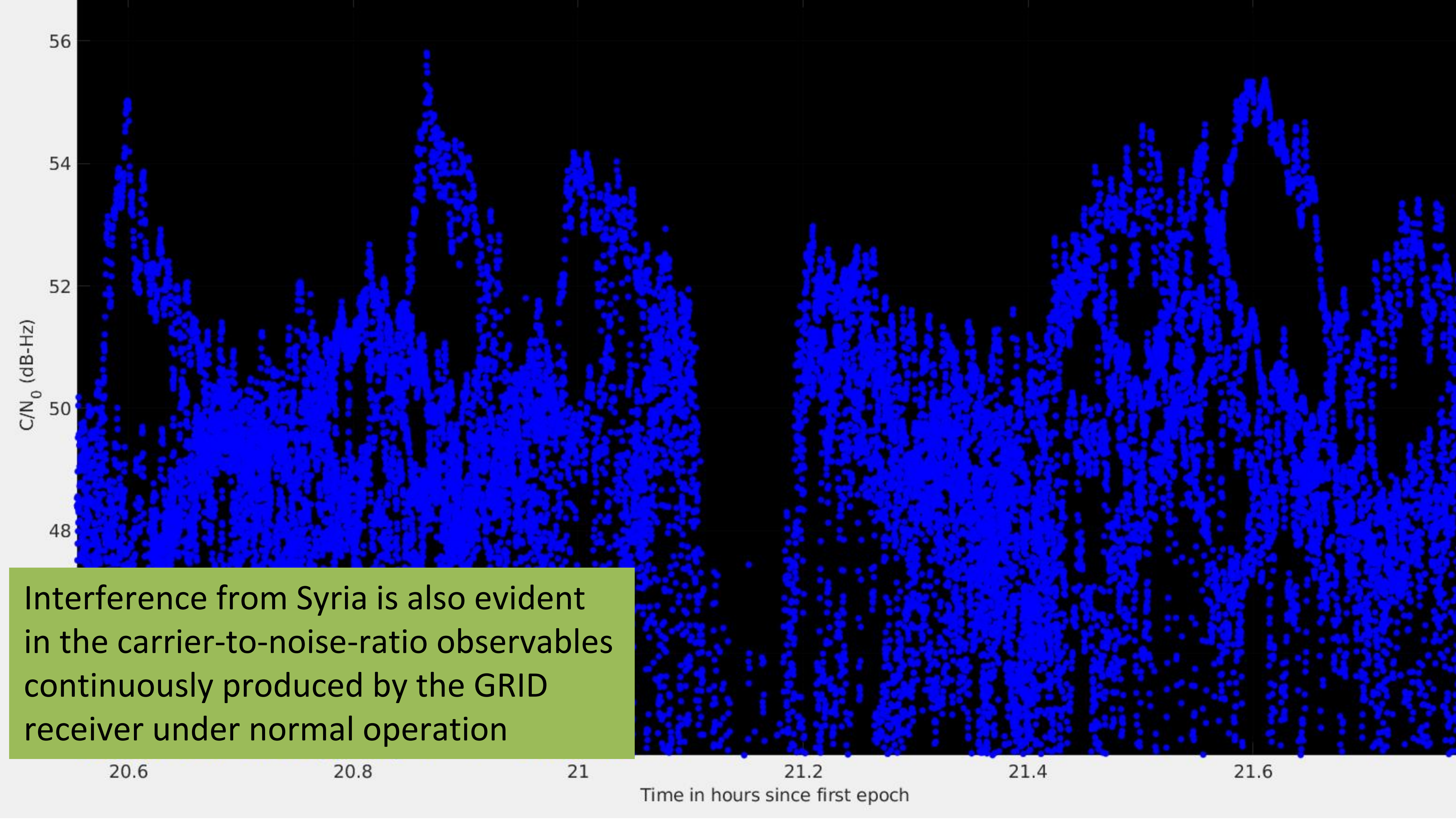


Khmeimim Air Base, Syria



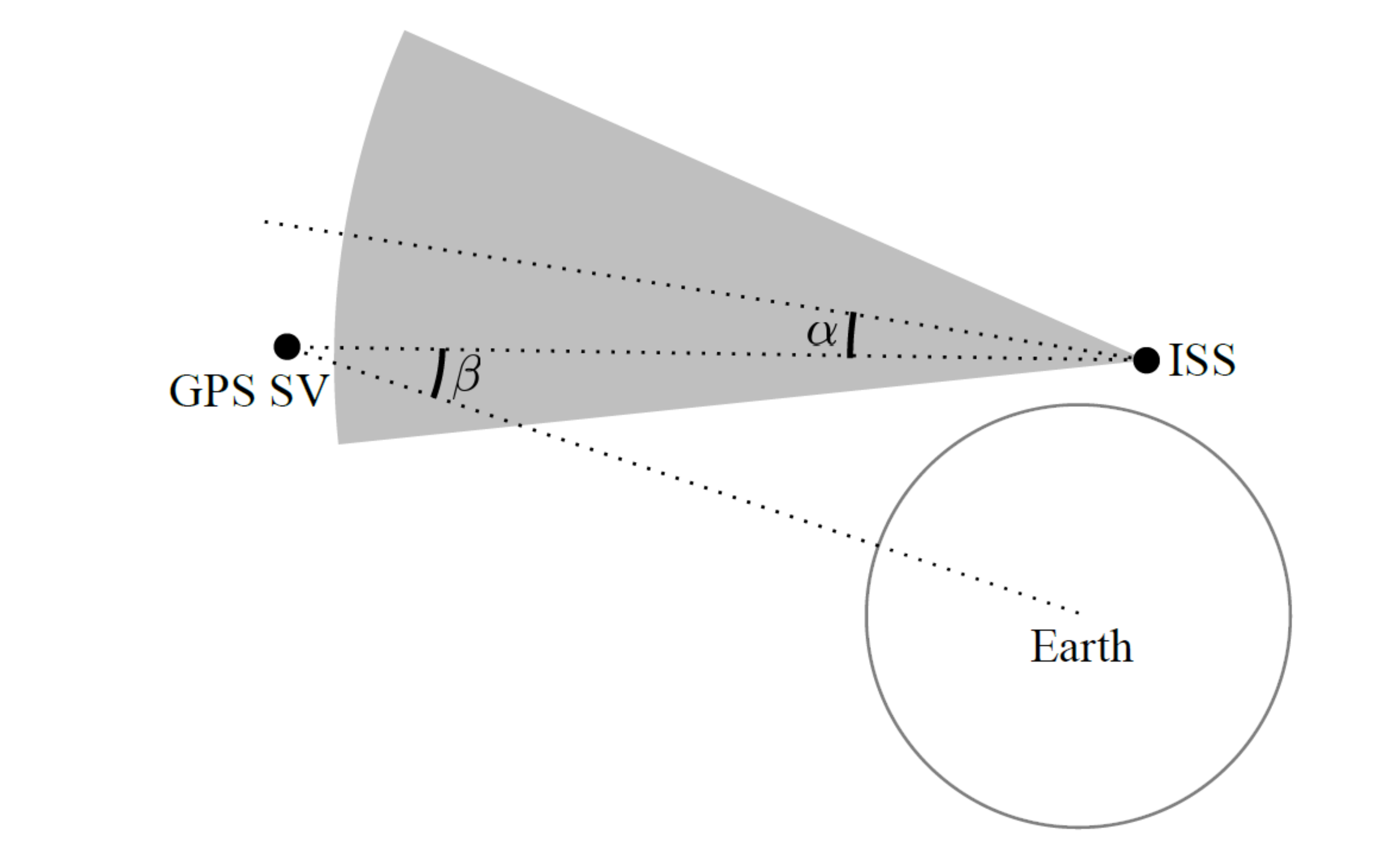
April 2018: “[Syria is] the most aggressive electronic warfare environment on the planet.”

Gen. Raymond Thomas, commander
U.S. Special Operations Command

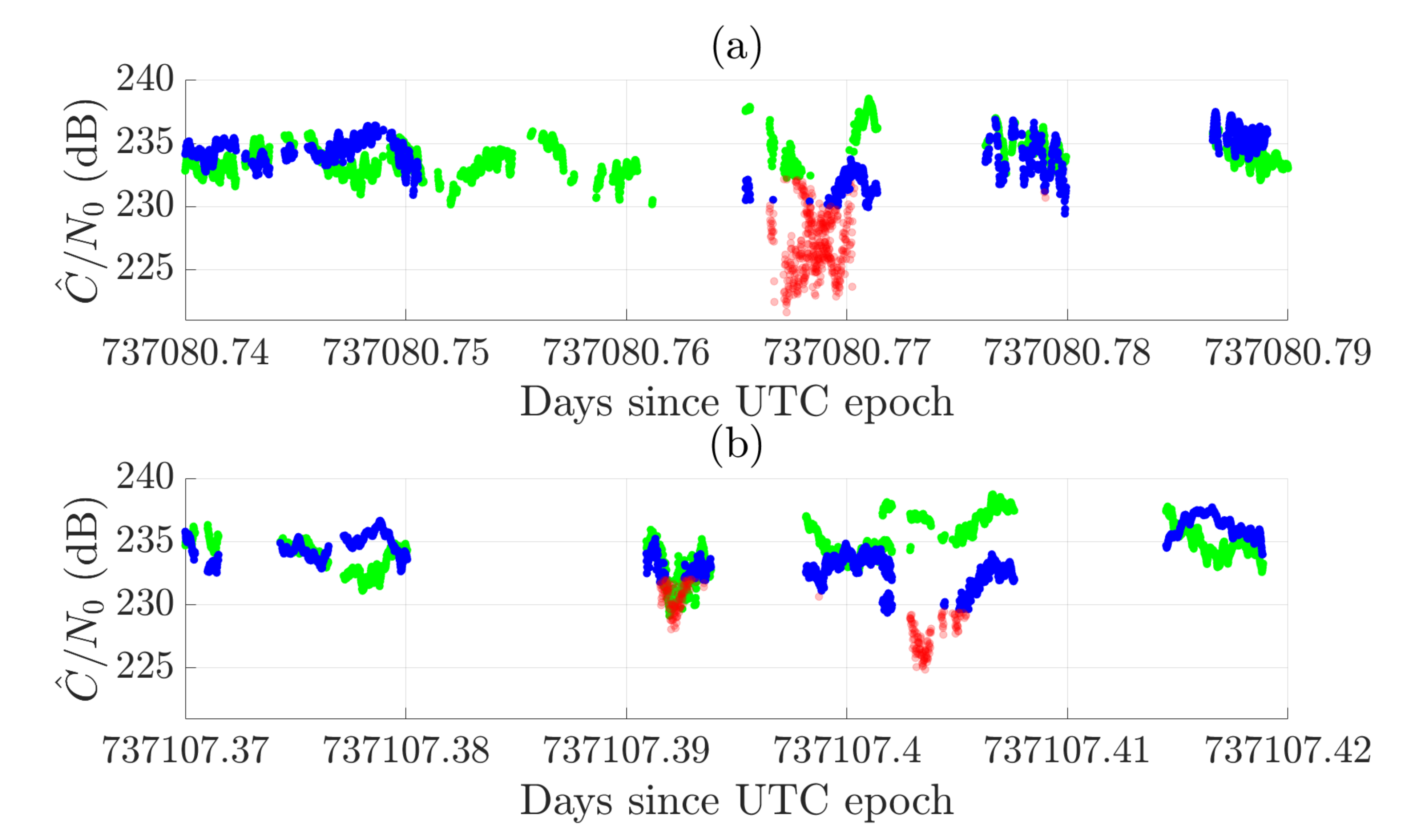


Interference from Syria is also evident in the carrier-to-noise-ratio observables continuously produced by the GRID receiver under normal operation

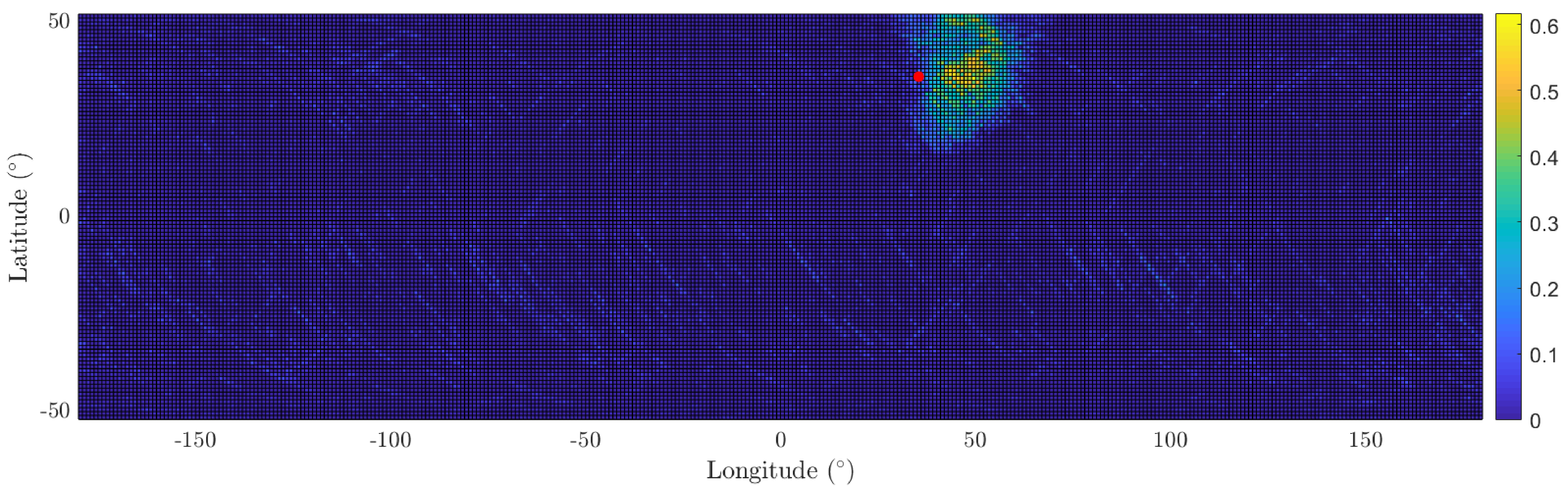
$$C(j, f, r_{sr}, z_s, z_r)$$



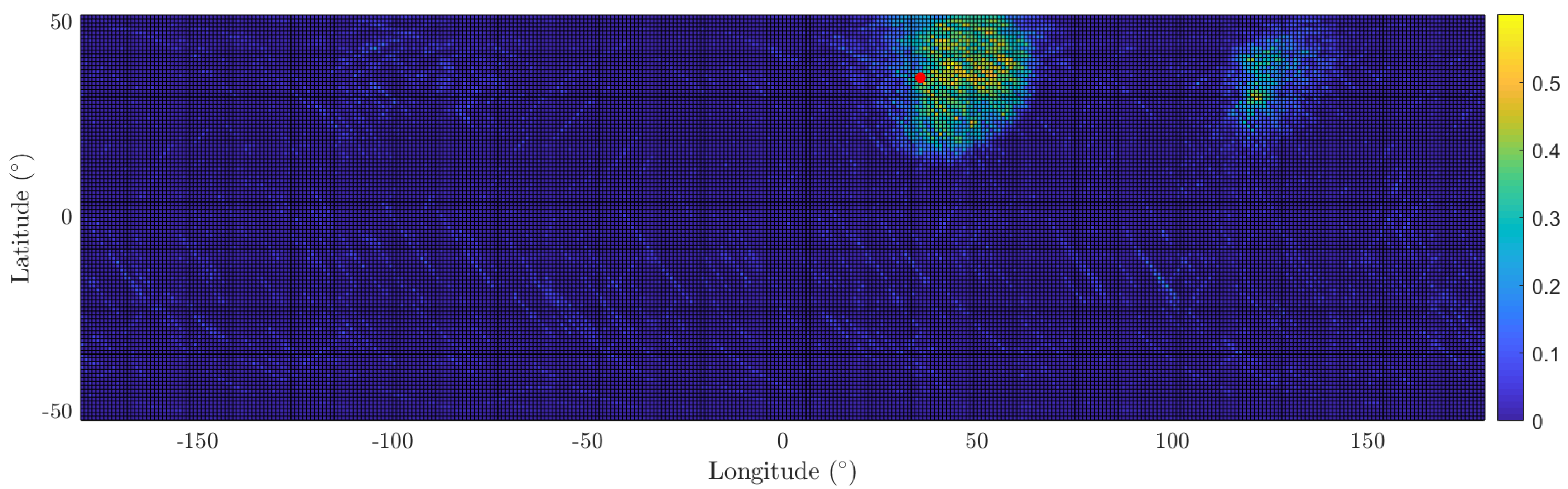
To maximize detectability, CINR observations must be pre-processed to compensate for predictable variations due to PRN (j), frequency (f), range (r_{sr}), satellite off-boresight angle (z_s), and receiver off-boresight angle (z_r).



Model-compensated receiver-reported CINR as ISS overflies interference zones



Heat map based on standard 1-Hz L1 C/N0 data from ISS GRID receiver from Jan–Nov 2018. The interference source in Syria is clearly evident, with a pattern asymmetry due to the receiver's antenna pointing aft.

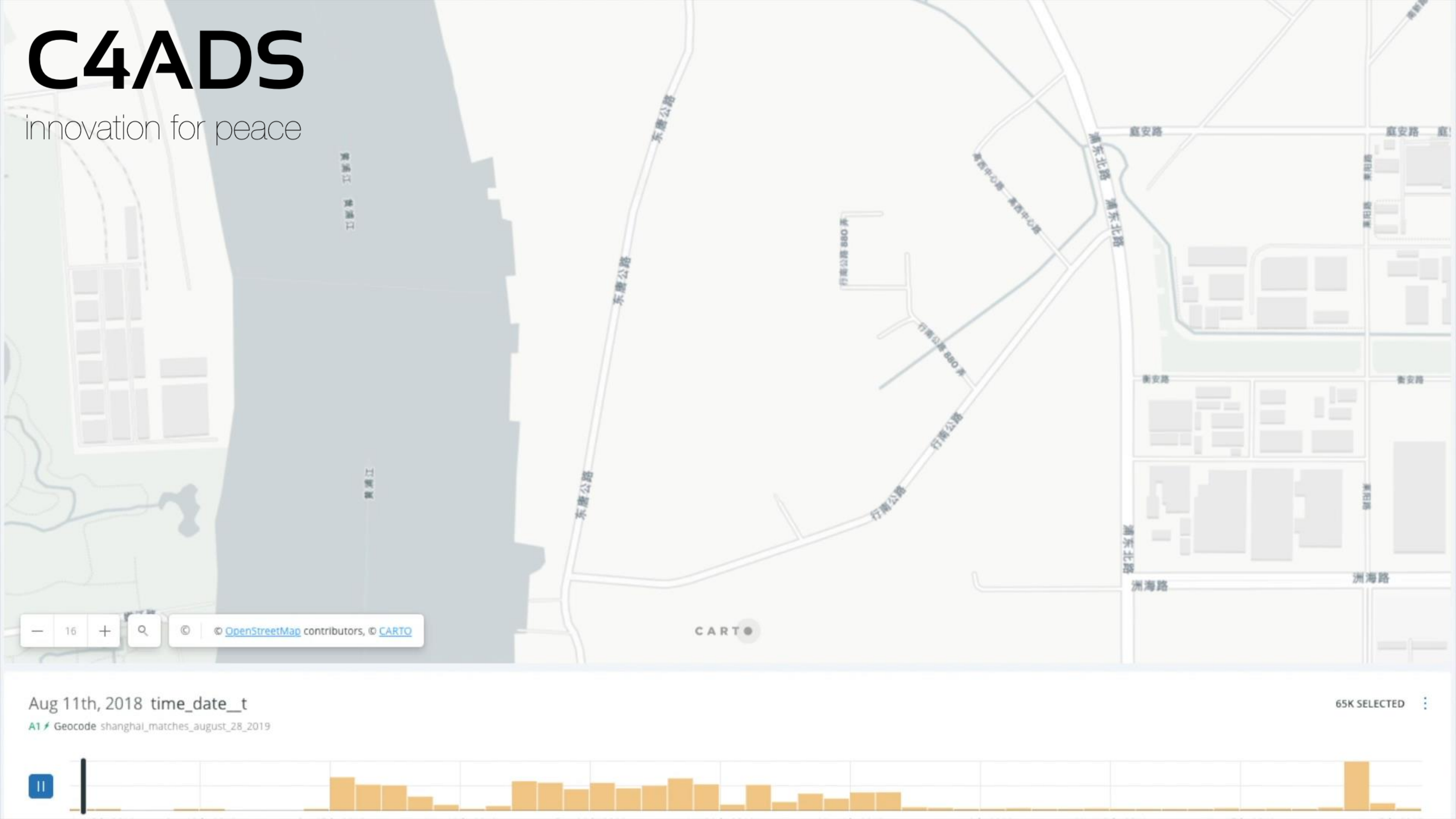


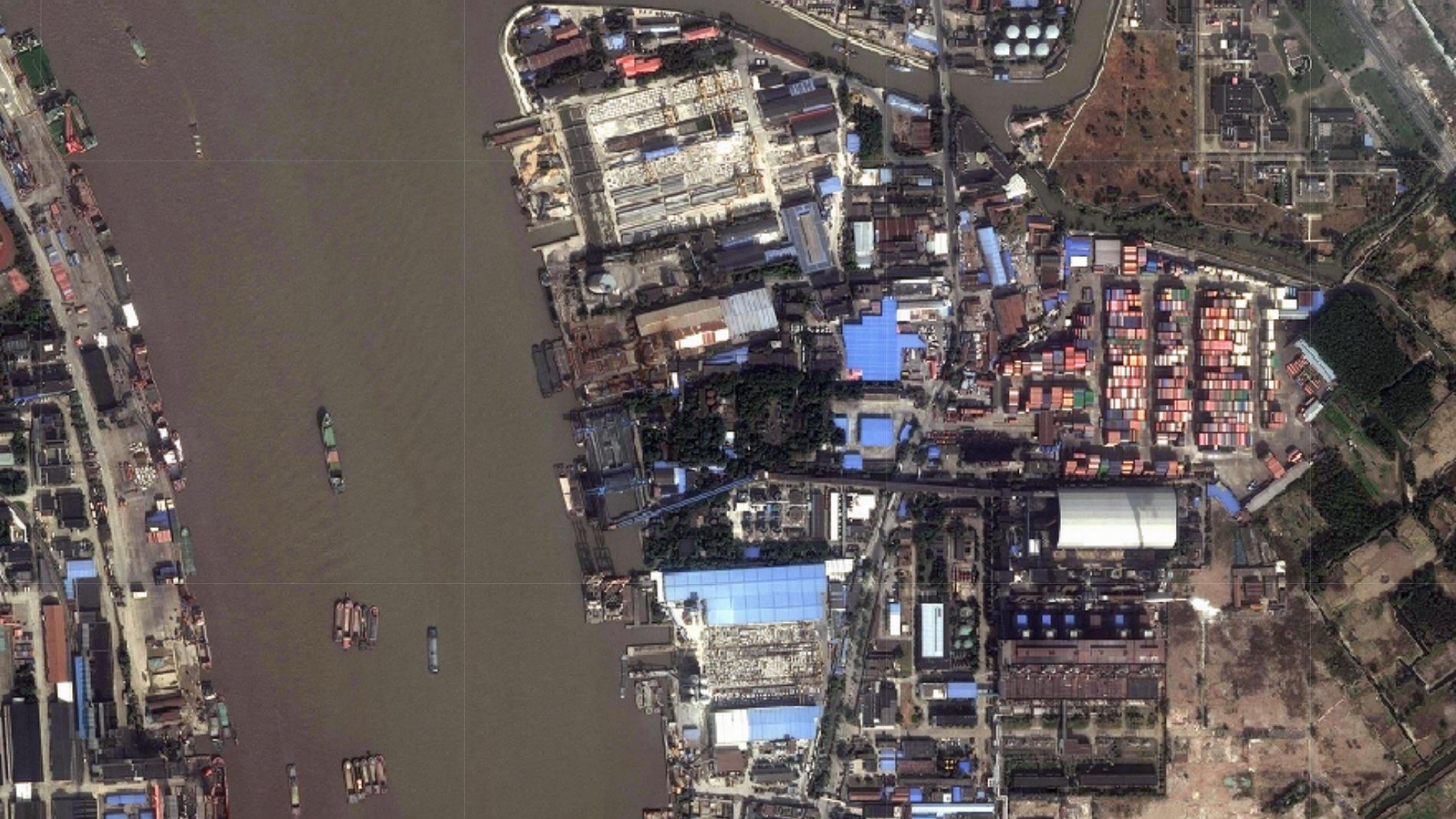
Heat map based on standard 1-Hz L2 C/N0 data from ISS GRID receiver from Jan–Nov 2018. Interference from Syria is evident, as is a persistent signature south of Gobi desert.

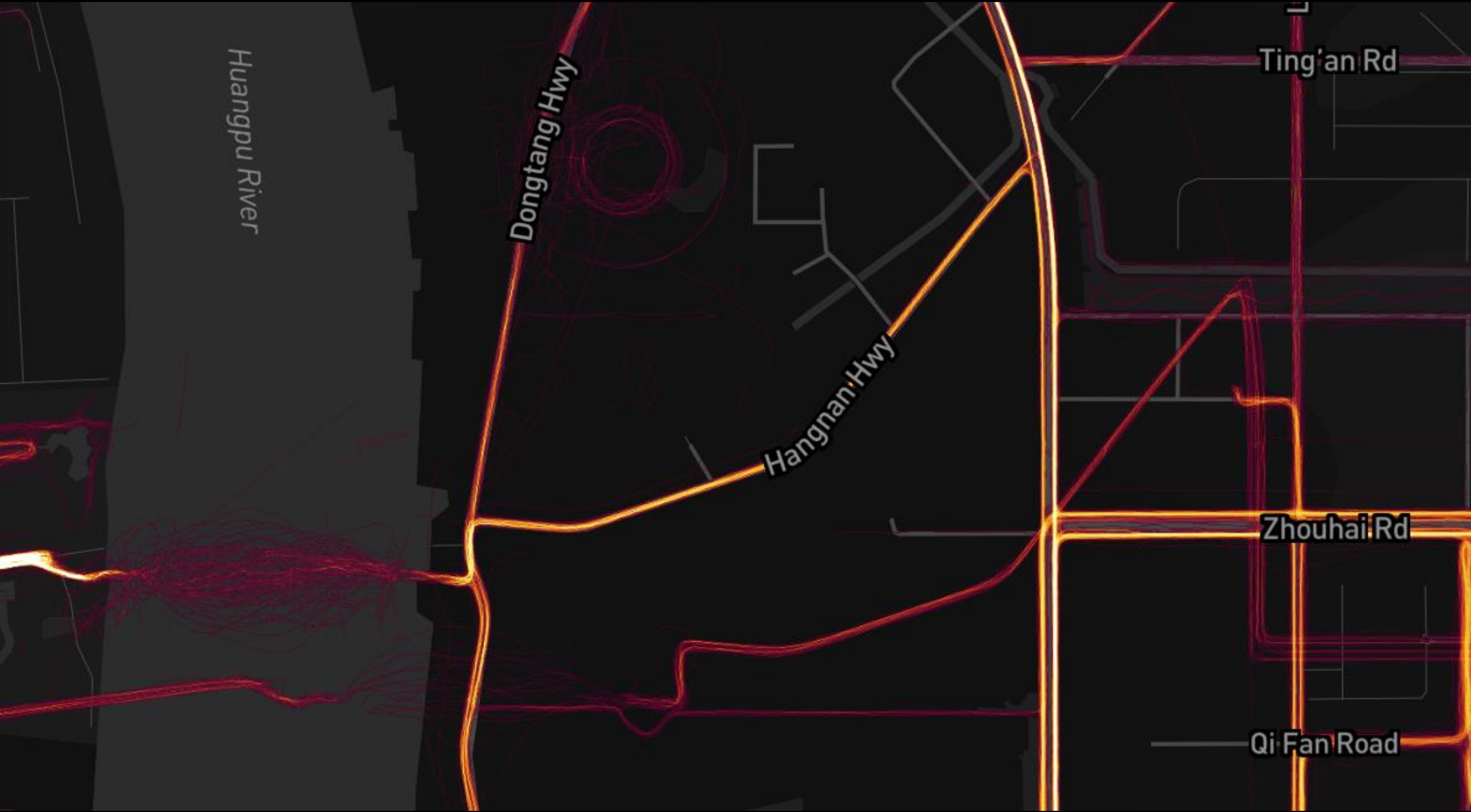

Port of Shanghai: Oct. 2018 -- Aug. 2019

C4ADS

innovation for peace






Huangpu River
Dongtang Hwy
Ting'an Rd
Hangnan Hwy
Zhouhai Rd
Qi Fan Road


Dongtang Hwy

Insights (1/2):

a) Russia and China are engaged in wide-area GNSS spoofing and jamming in multiple locations
b) Improved spoofing detection without improved spoofing resilience opens the door to spoofing for denial of service
c) Against civil receivers performing cold start, spoofing is more efficient for denial of service than jamming: a 1W spoofer is more potent than a 1kW narrow/wideband jammer at the same stand-off distance
d) Cold start remains a necessary capability for many applications of interest

Insights (2/2):

a) A science-grade GNSS receiver in LEO is a power tool for global GNSS interference monitoring
b) Detection of signals as weak as 3.5 dBW (via CINR) and and -28.5 dBW (via acquisition) is possible in theory
c) Localization of terrestrial sources is possible to better than a few km
d) We detected wide-area persistent GNSS interference in two locations
e) Interference from Syria is matched-code: potent for DoS

THE UNIVERSITY OF TEXAS AT AUSTIN

RADIONAVIGATION LABORATORY