THE UNIVERSITY OF TEXAS AT AUSTIN
RADIONAVIGATION LABORATORY

GNSS Radio Frequency Interference Detection from LEO

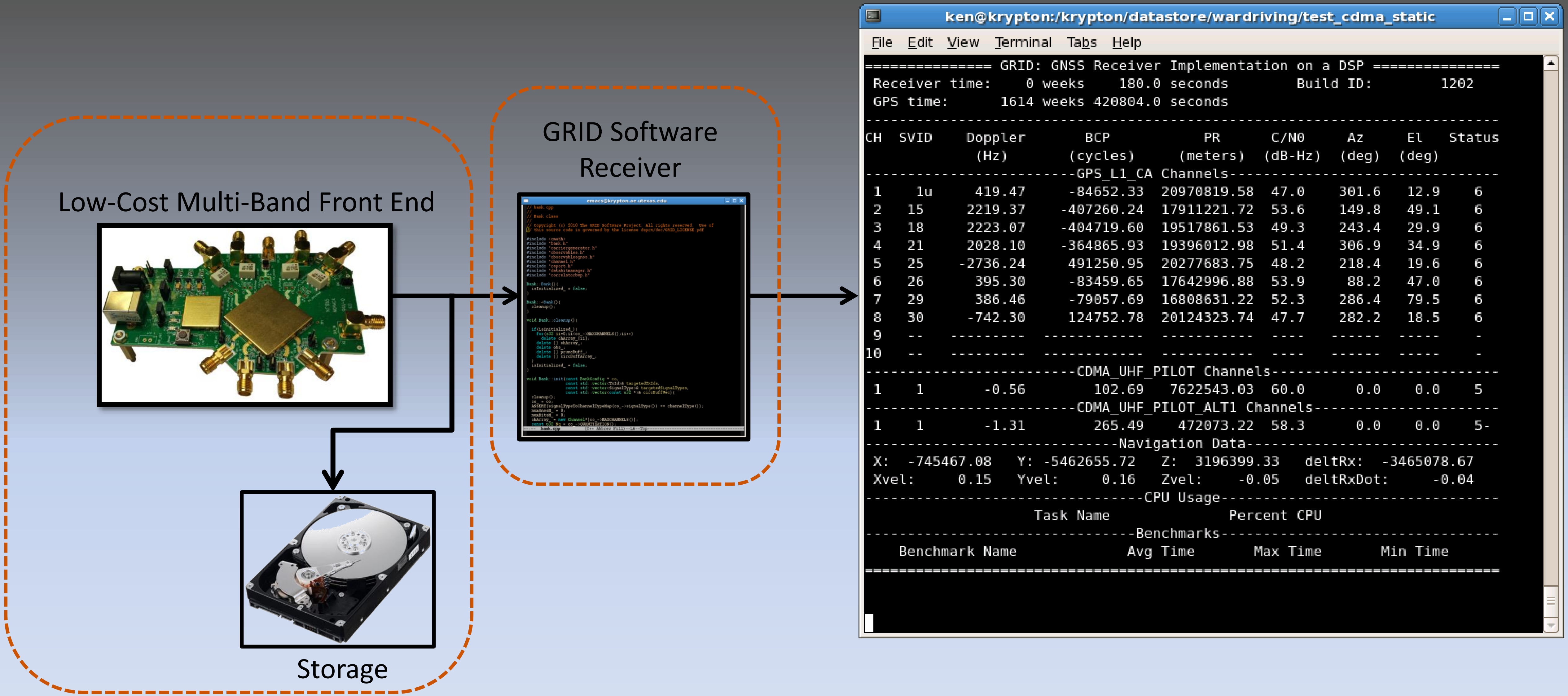
Todd Humphreys

In collaboration with Matthew Murrian, Lakshay Narula, Peter Iannucci, Scott Budzien (NRL), and C4ADS

Department of Aerospace Engineering and Engineering Mechanics

The University of Texas at Austin

PNT EXCOM Advisory Board Semi-Annual Meeting | June 6, 2019



Software-defined radio is a key asset for agile and assured PNT.
The University of Texas GRID receiver is the result of 12 years' development.

February 2017: GRID 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.

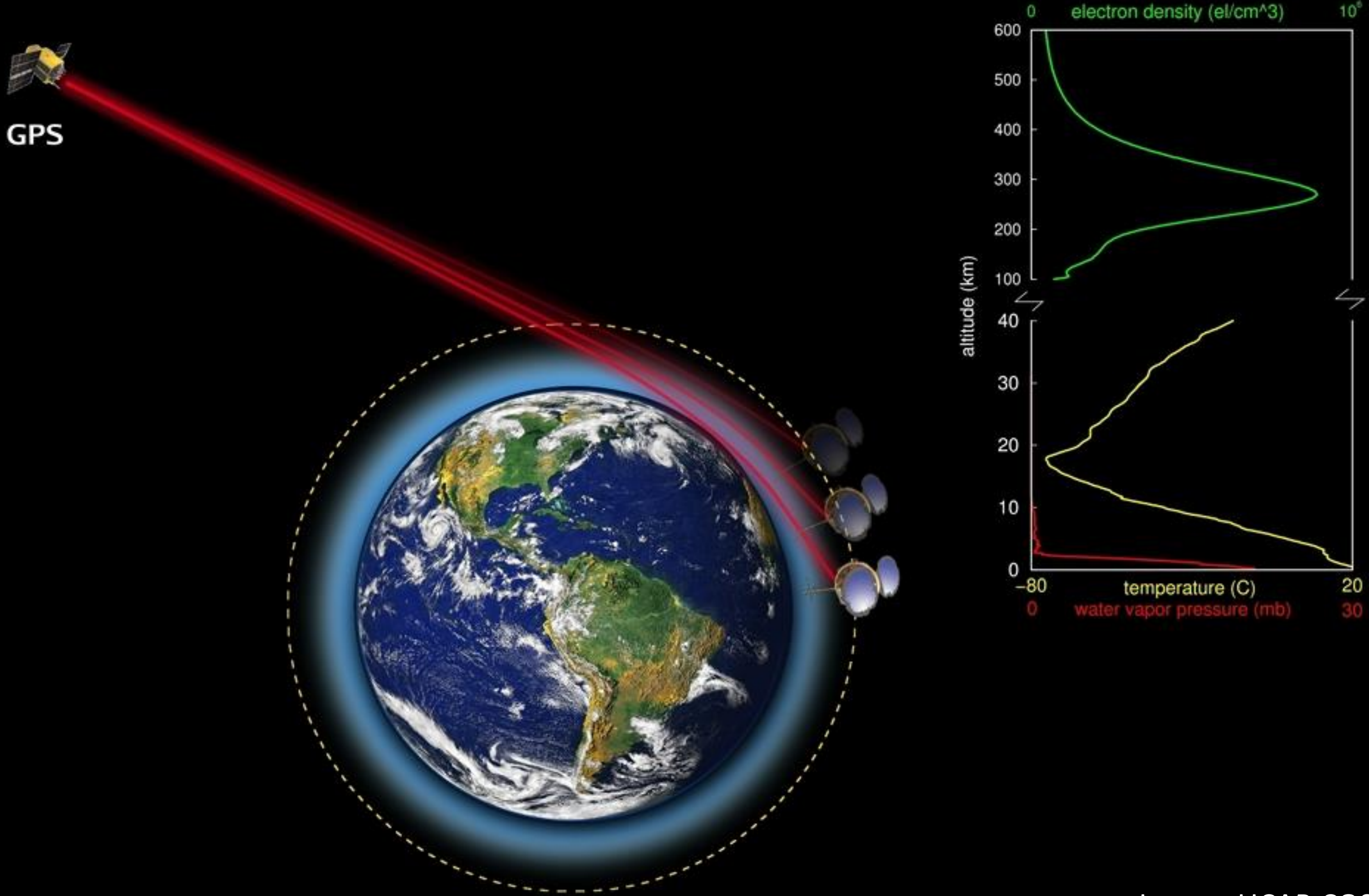
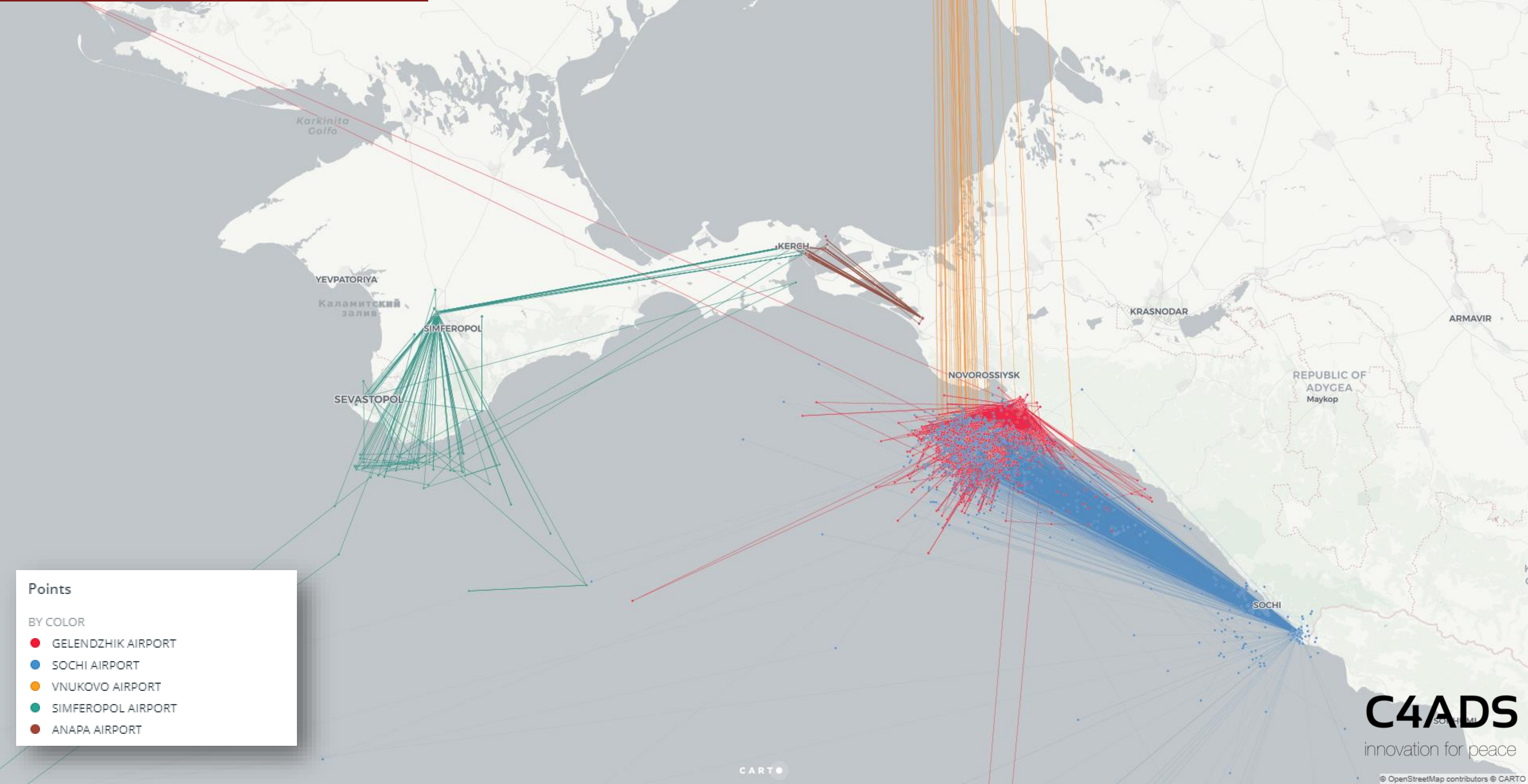


Image: UCAR COSMIC Program

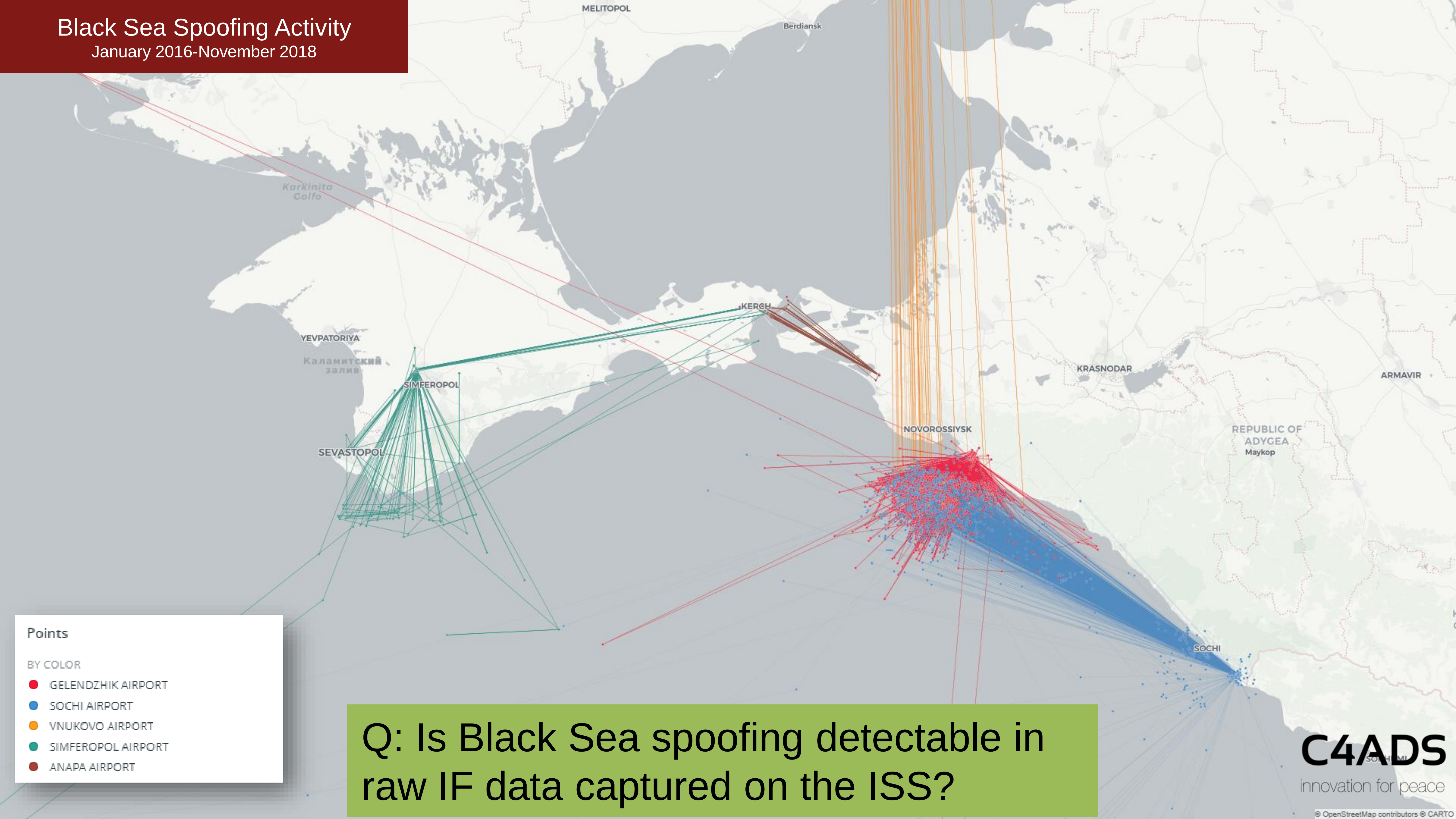
Black Sea Spoofing Activity
January 2016-November 2018



C4ADS
innovation for peace

Black Sea Spoofing Activity

January 2016-November 2018



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

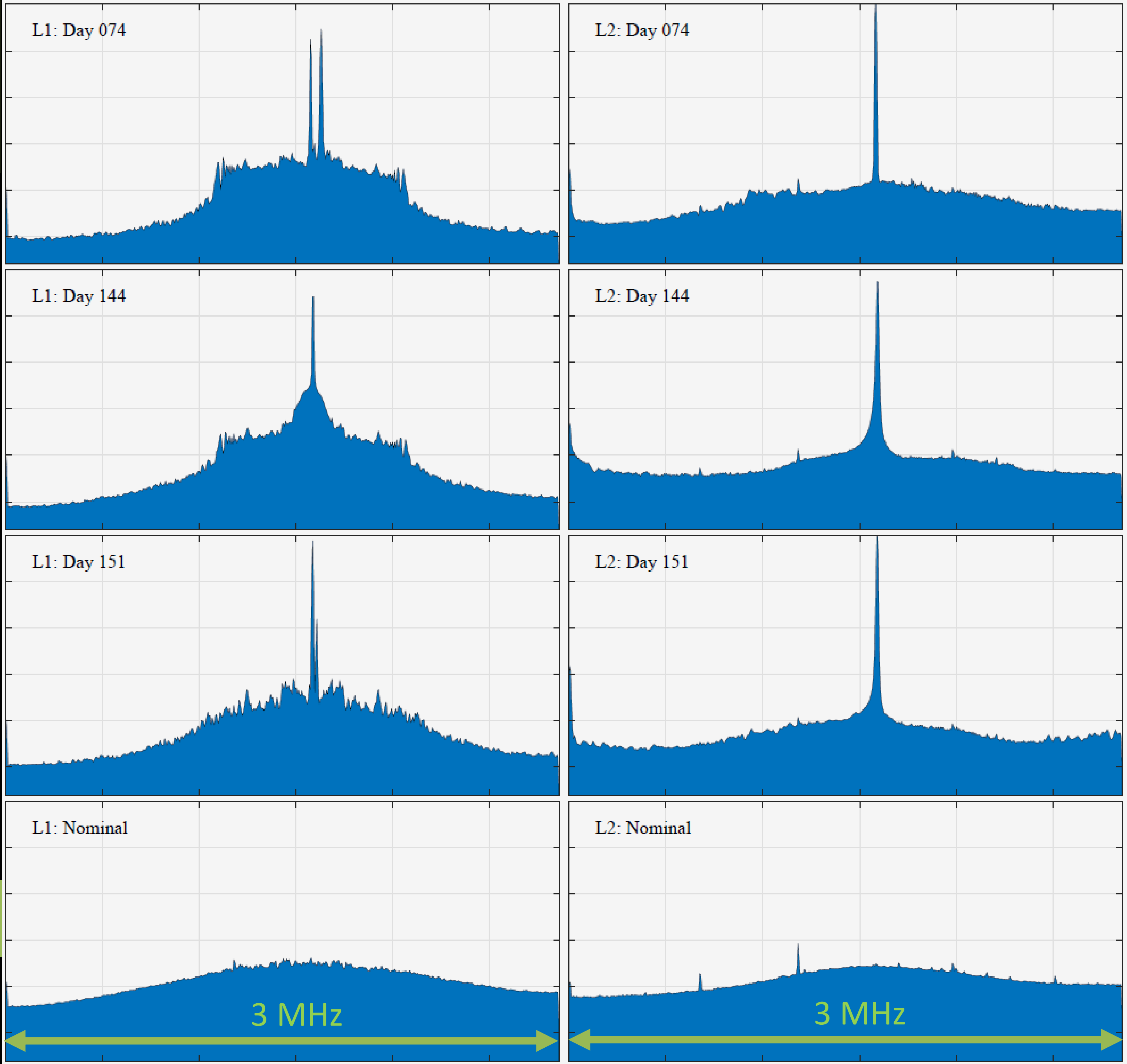
C4ADS

innovation for peace

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

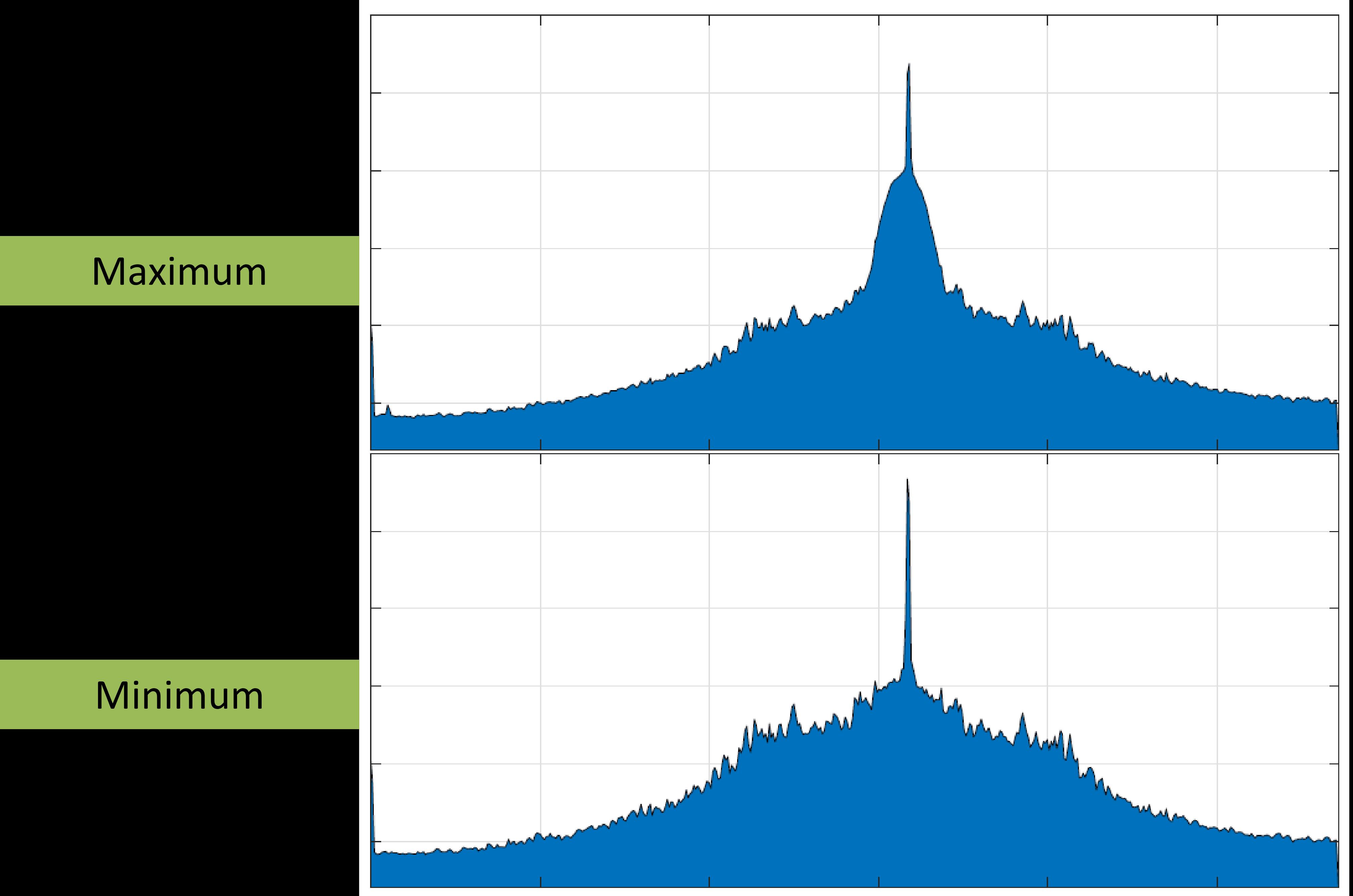
60-second recordings sent via NASA's communications backbone to NRL and thence to UT for processing with latest version of GRID

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

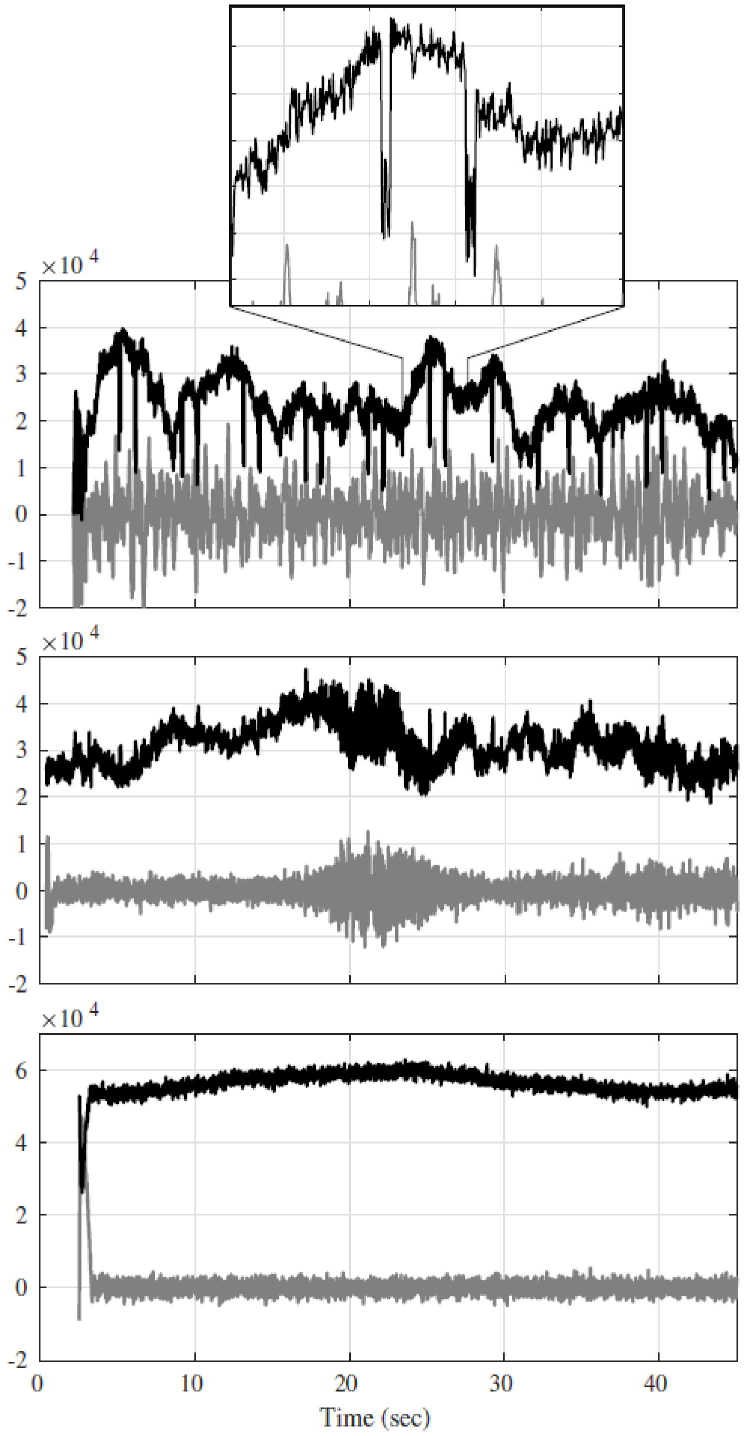
Data-Wiped 100-Hz IQ accumulations

Unexplained fading

False signal

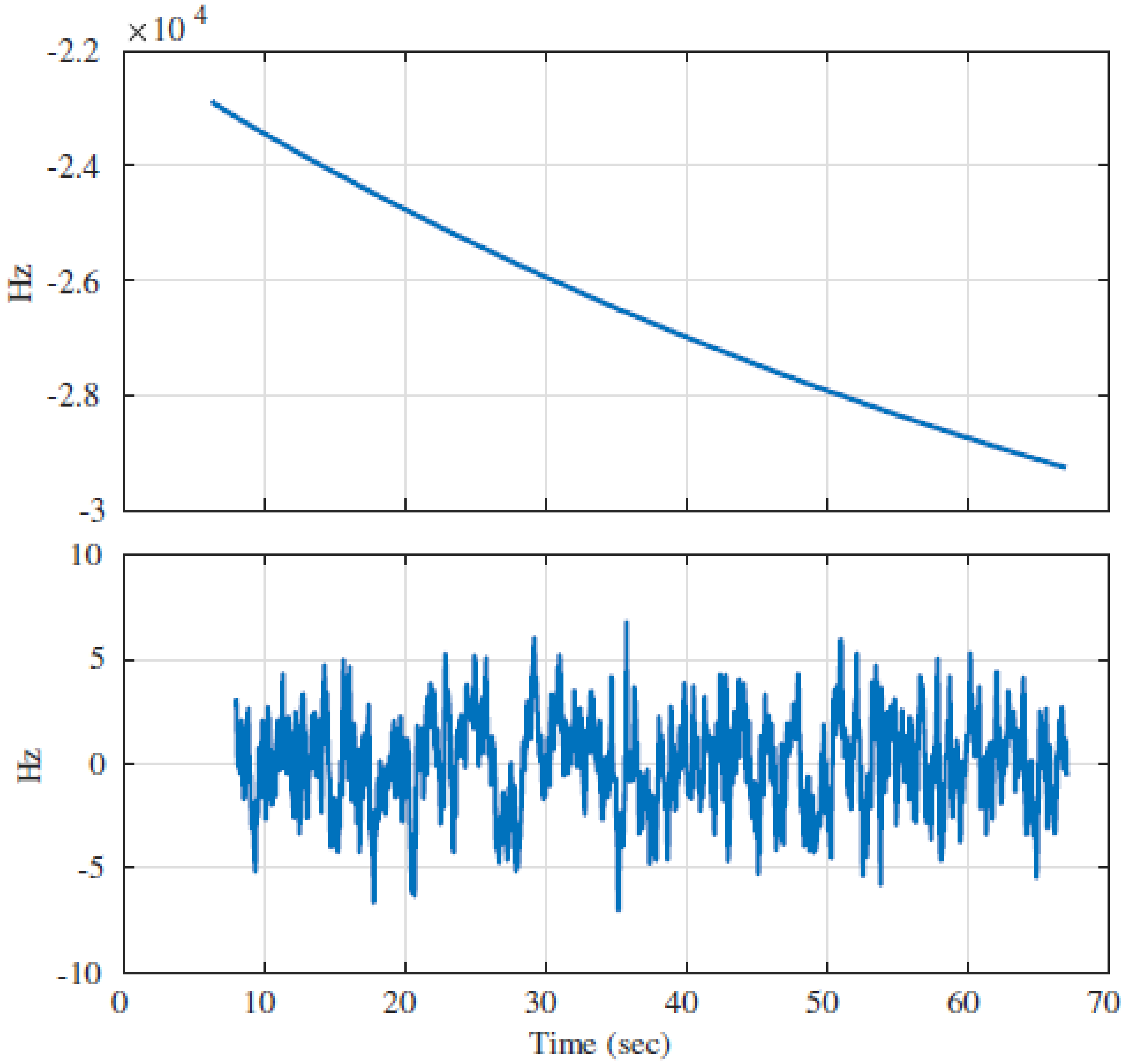
Authentic signal in interference

Authentic signal under clean conditions



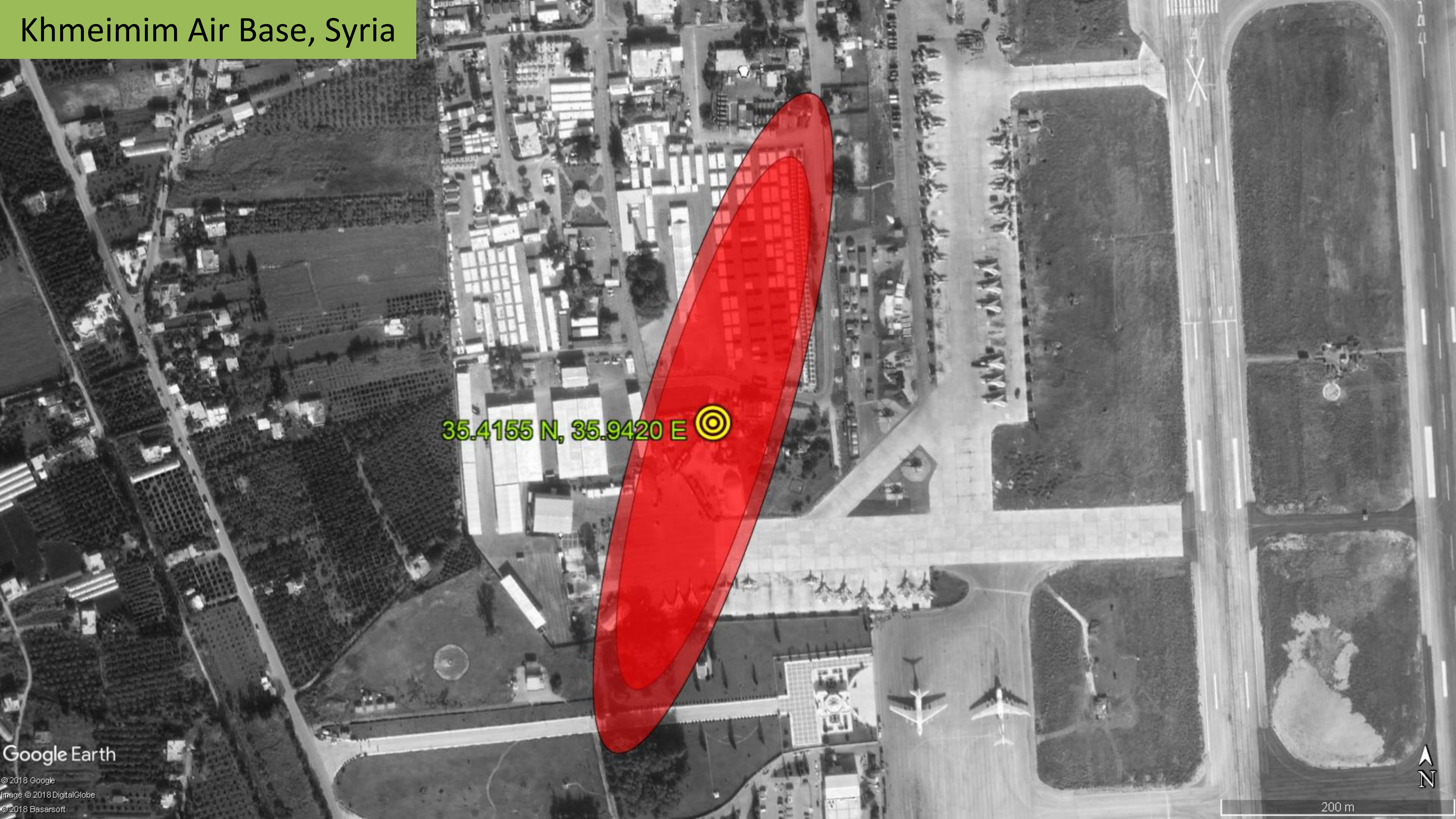
Doppler time history for false PRN 10 signal from day 144 capture

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

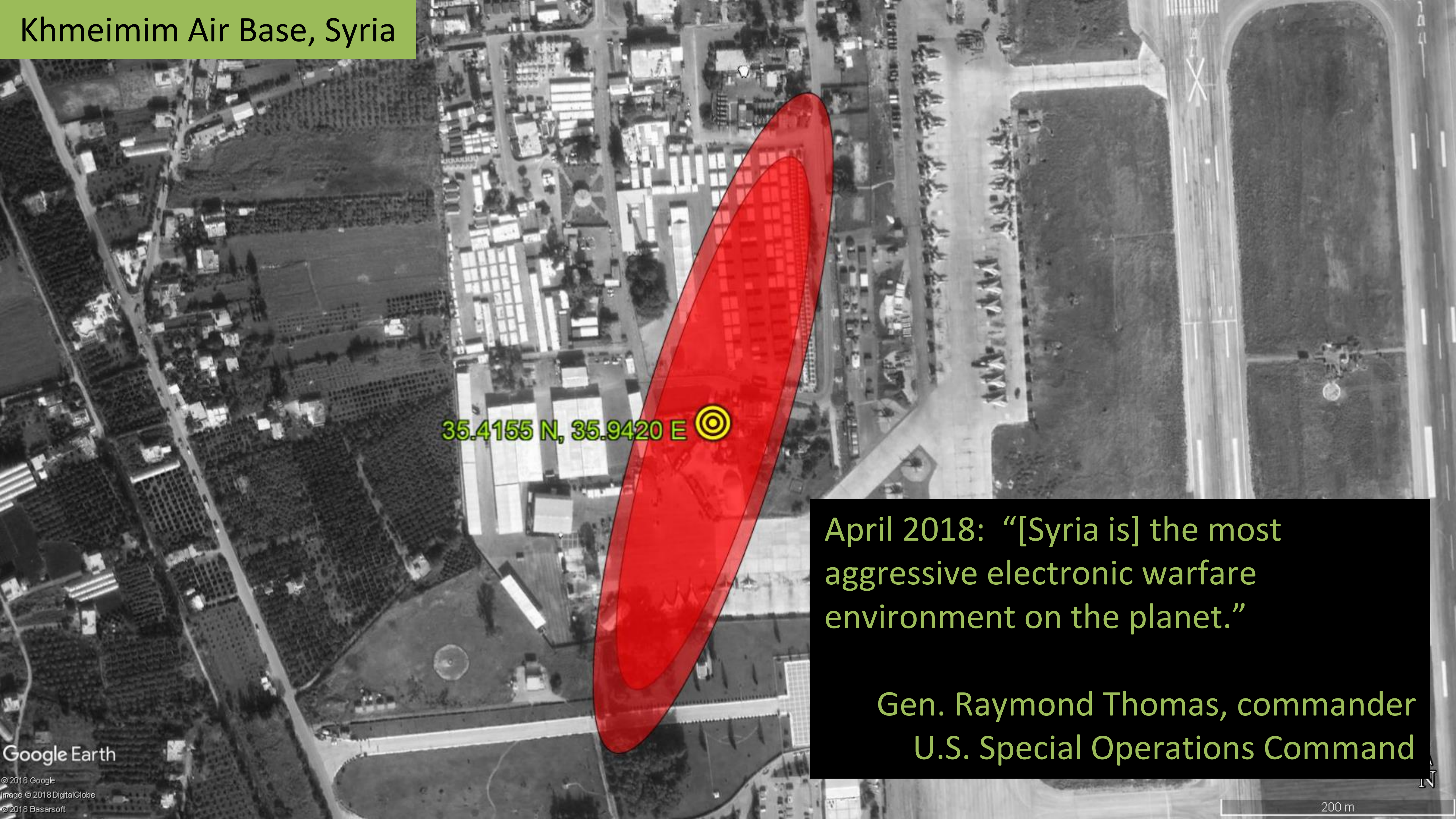


Doppler time histories can be used to infer transmitter location, assuming a transmitter clock with a constant frequency offset over each 60-second interval

Khmeimim Air Base, Syria

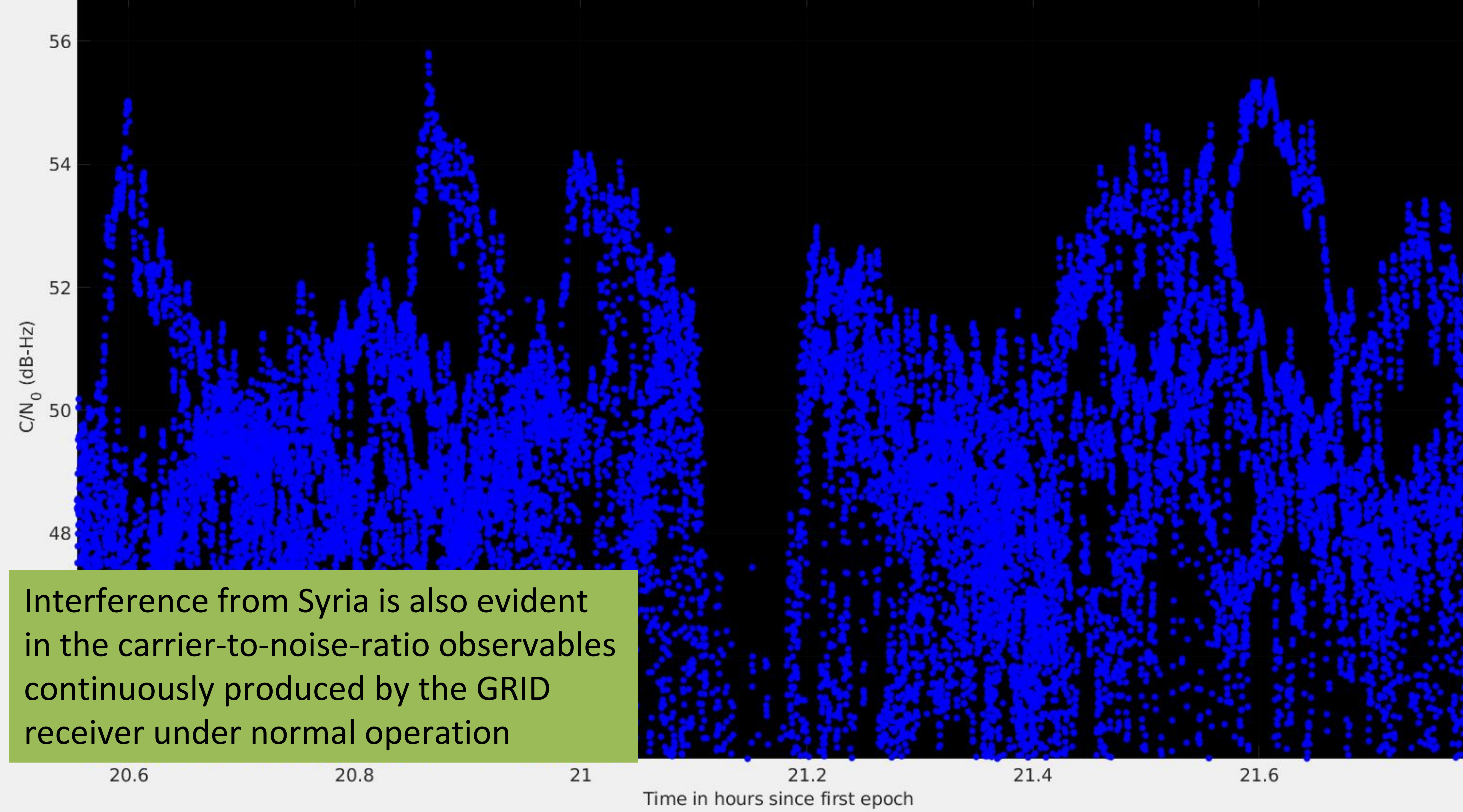


Khmeimim Air Base, Syria

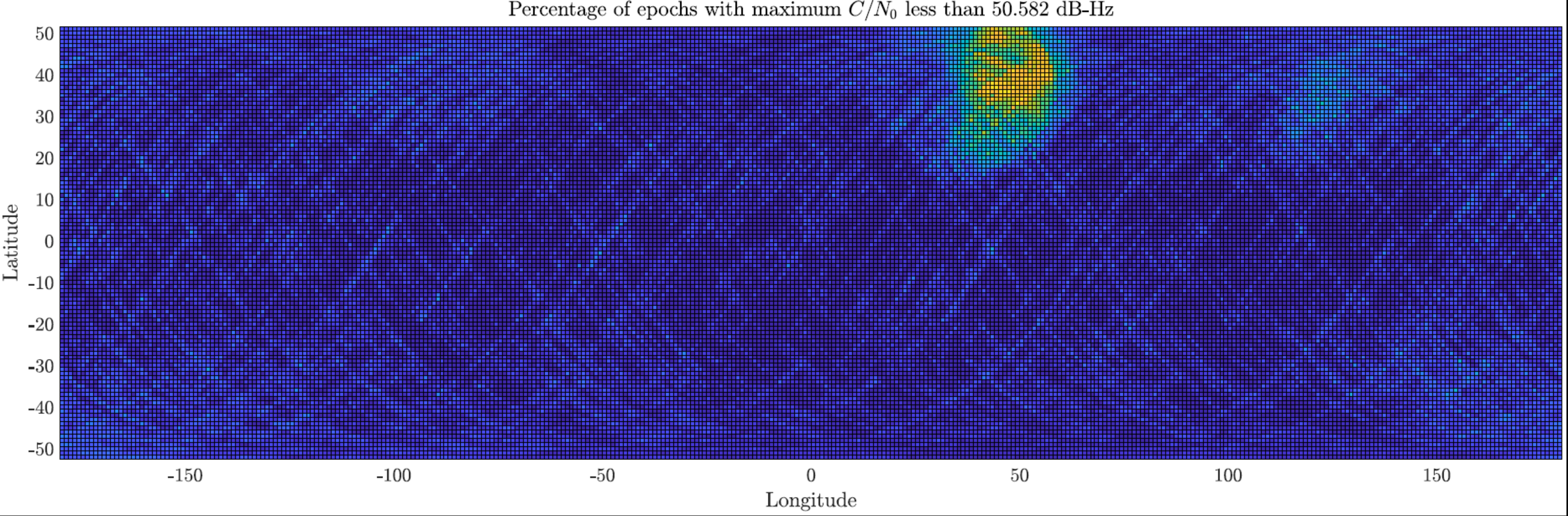


April 2018: "[Syria is] the most aggressive electronic warfare environment on the planet."

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



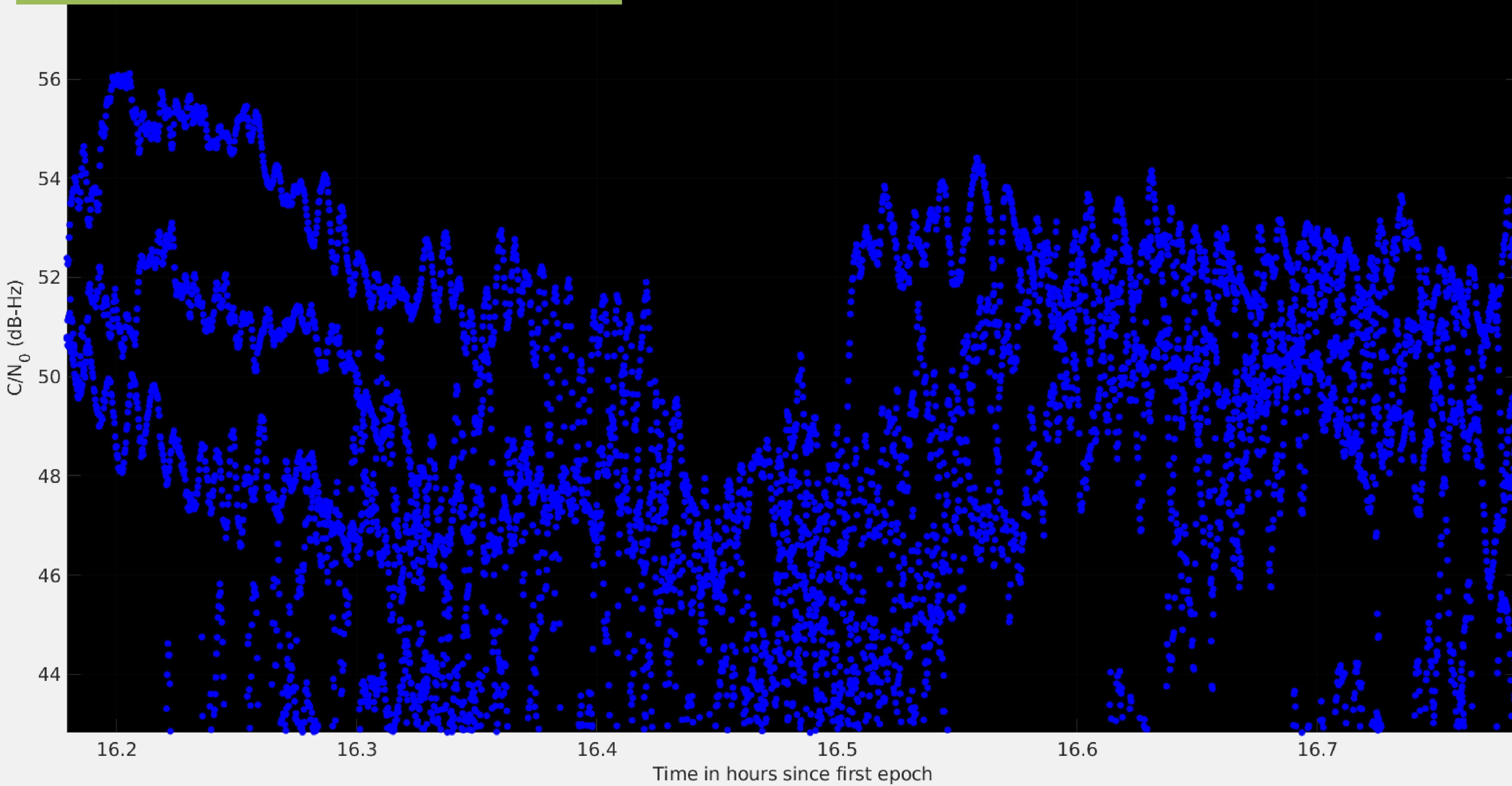
Interference from Syria is also evident in the carrier-to-noise-ratio observables continuously produced by the GRID receiver under normal operation

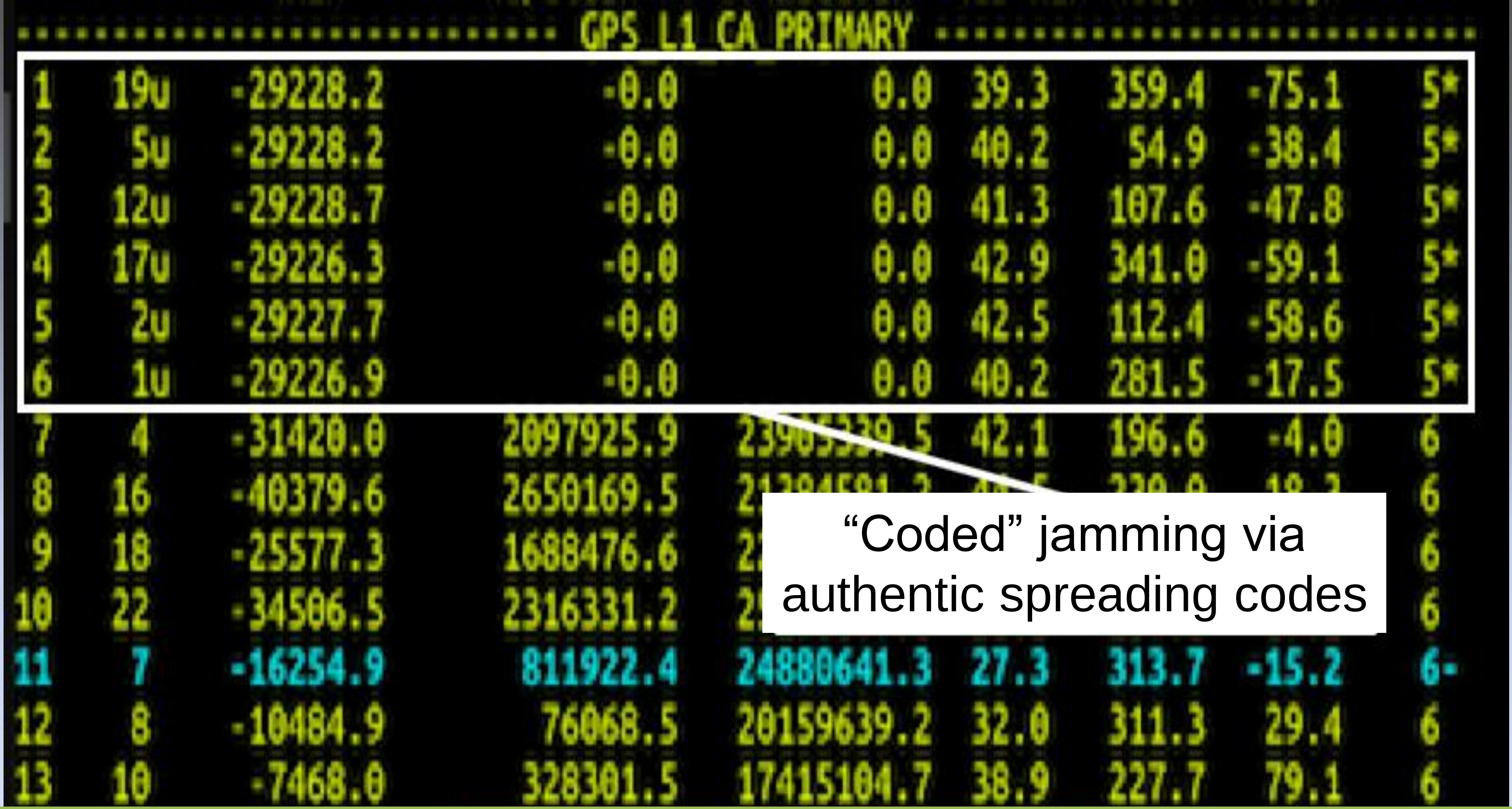


Heat map based on standard 1-Hz C/N0 data from ISS GRID receiver from Jan–Nov 2018. The interference source in Syria is clearly evident, with a pattern asymmetry due to the receiver's antenna pointing aft.

Interference activity also appears in Asia and possibly around New Zealand.

Suspected interference event in Asia





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).

Observations:

a) Suitable LEO instruments can reveal scope, nature, and location of terrestrial GPS interference.

b) Against receivers performing cold start, spoofing is more efficient for denial of GPS than jamming: a 1W spoofer is more potent than a 1kW narrow/wideband jammer at the same stand-off distance.

c) Goals for protecting and toughening GPS that are stated in terms of J/S (e.g., 85 dB J/S to withstand a 1kW jammer at a distance of 2 km) assume uncorrelated jamming, not spoofing.

d) Cold start remains a necessary capability for many applications of interest.

THE UNIVERSITY OF TEXAS AT AUSTIN
RADIONAVIGATION LABORATORY