



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

Low-Cost Multi-Band Front End



Storage

GRID Software Receiver

```
emacs@krypton.as.utexas.edu
// main.cpp
// main class
// Copyright (c) 2010 The GRID Software Project. All rights reserved. Use of
// this source code is governed by the license docs/GRID_LICENSE.pdf

#include <cmath>
#include "receiveroperator.h"
#include "observed.h"
#include "observedgps.h"
#include "channel.h"
#include "signal.h"
#include "signalmanager.h"
#include "observedcdma.h"

Grid::Grid()
    initialized_( false )
{
}

Grid::~Grid()
{
    cleanup();
}

void Grid::cleanup()
{
    if( !initialized_ )
        return;
    delete observed_;
    delete observedgps_;
    delete channel_;
    delete signal_;
    delete signalmanager_;
    delete observedcdma_;
    initialized_ = false;
}

void Grid::init(const GridConfig & c)
{
    const GridConfig & c = c;
    const GridConfig & c = c;
    const GridConfig & c = c;
    const GridConfig & c = c;
    cleanup();
    c = c;
    addSignalTypesToChannels(c._signalTypes() == channelType());
    channels_ = 0;
    channels_ = new Channels(c._channels());
    channels_ = new Channels(c._channels());
    channels_ = new Channels(c._channels());
}

Grid::~Grid()
{
    cleanup();
}
```

```
ken@krypton:/krypton/datastore/warDriving/test_cdma_static
File Edit View Terminal Tabs Help

===== GRID: GNSS Receiver Implementation on a DSP =====
Receiver time: 0 weeks 180.0 seconds      Build ID: 1202
GPS time: 1614 weeks 420804.0 seconds

-----
CH  SVID   Doppler      BCP          PR          C/N0        Az          El          Status
(Hz)      (cycles)      (meters)      (dB-Hz)      (deg)      (deg)
-----
-----GPS_L1_CA Channels-----
1    1u     419.47       -84652.33    20970819.58  47.0        301.6       12.9        6
2    15     2219.37      -407260.24   17911221.72  53.6        149.8       49.1        6
3    18     2223.07      -404719.60   19517861.53  49.3        243.4       29.9        6
4    21     2028.10      -364865.93   19396012.98  51.4        306.9       34.9        6
5    25     -2736.24     491250.95    20277683.75  48.2        218.4       19.6        6
6    26     395.30       -83459.65    17642996.88  53.9        88.2        47.0        6
7    29     386.46       -79057.69    16808631.22  52.3        286.4       79.5        6
8    30     -742.30      124752.78    20124323.74  47.7        282.2       18.5        6
9    --     -----
10   --     -----
-----CDMA_UHF_PILOT Channels-----
1    1       -0.56        102.69       7622543.03   60.0        0.0         0.0         5
-----CDMA_UHF_PILOT_ALT1 Channels-----
1    1       -1.31        265.49       472073.22    58.3        0.0         0.0         5
-----Navigation Data-----
X: -745467.08  Y: -5462655.72  Z: 3196399.33  deltrX: -3465078.67
Xvel: 0.15    Yvel: 0.16     Zvel: -0.05   deltrXdot: -0.04
-----CPU Usage-----
Task Name          Percent CPU
-----Benchmarks-----
Benchmark Name     Avg Time          Max Time          Min Time
=====
```

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.



GPS

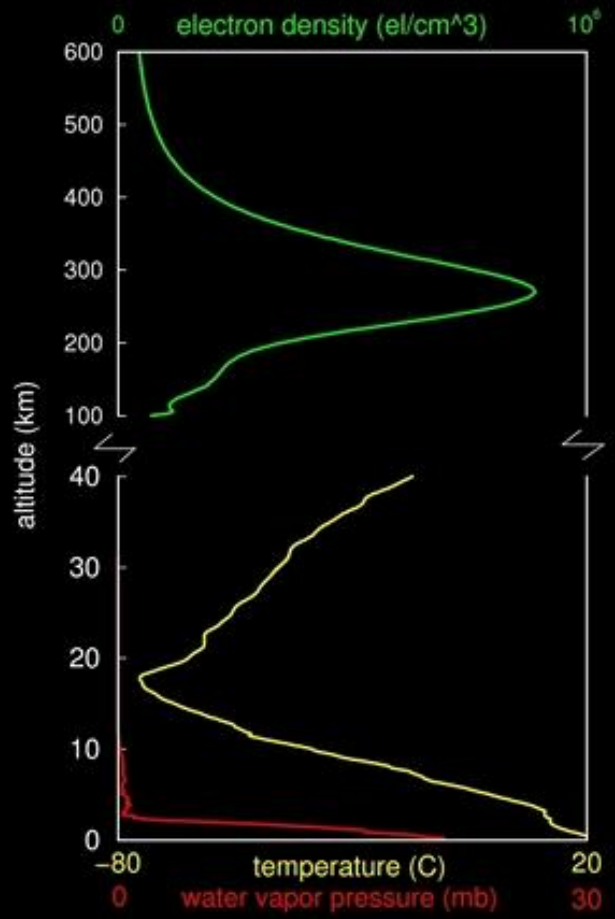
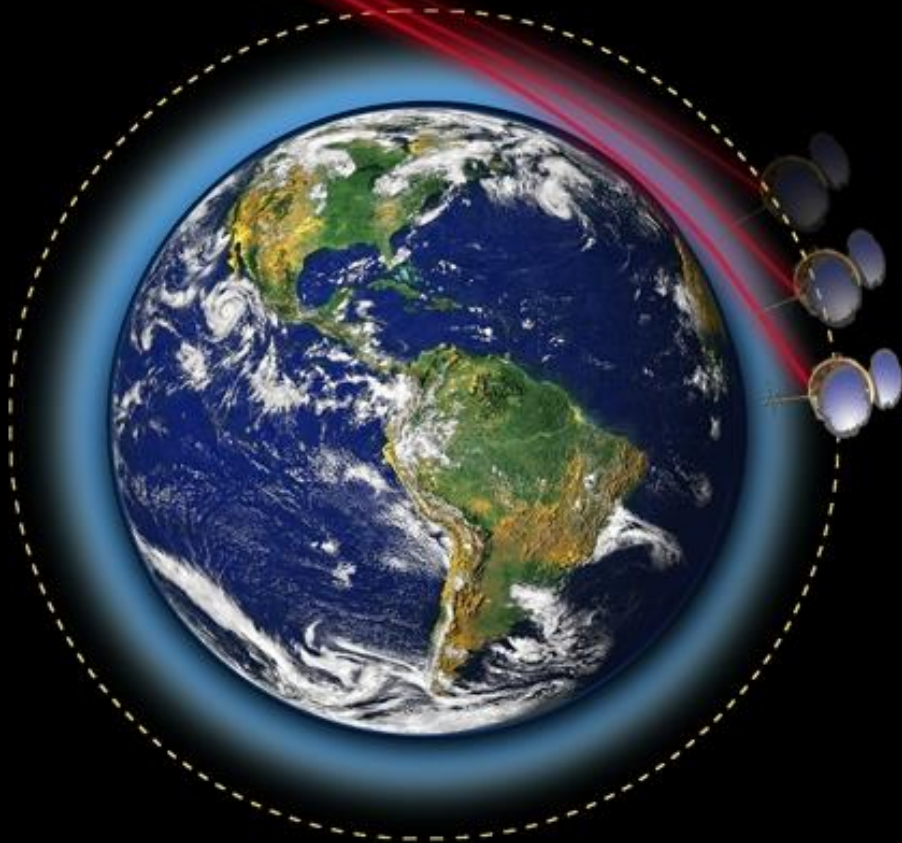


Image: UCAR COSMIC Program

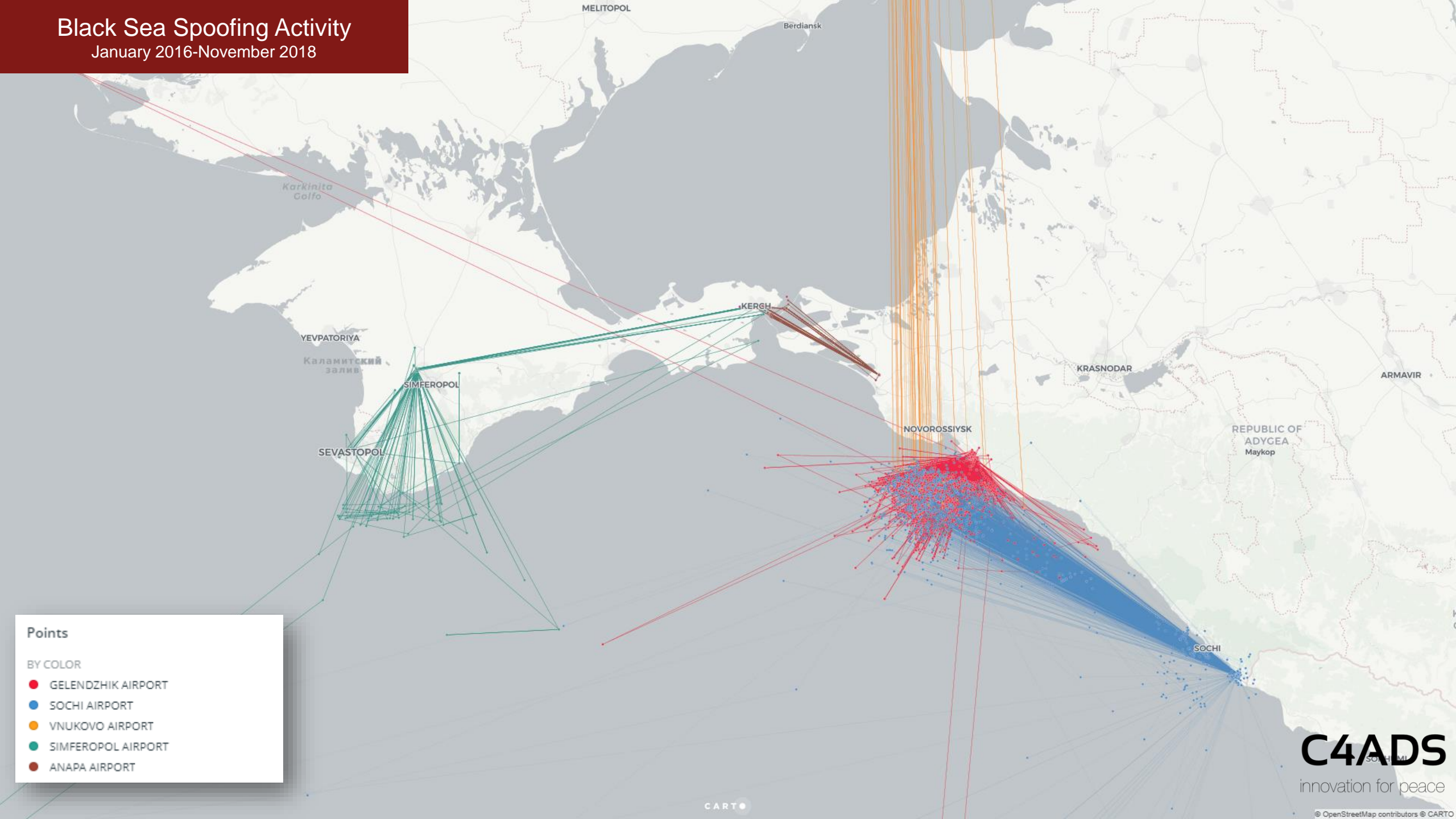
Black Sea Spoofing Activity

January 2016-November 2018

Points

BY COLOR

- GELENDZHIC AIRPORT
- SOCHI AIRPORT
- VNUKOVO AIRPORT
- SIMFEROPOL AIRPORT
- ANAPA AIRPORT



Black Sea Spoofing Activity

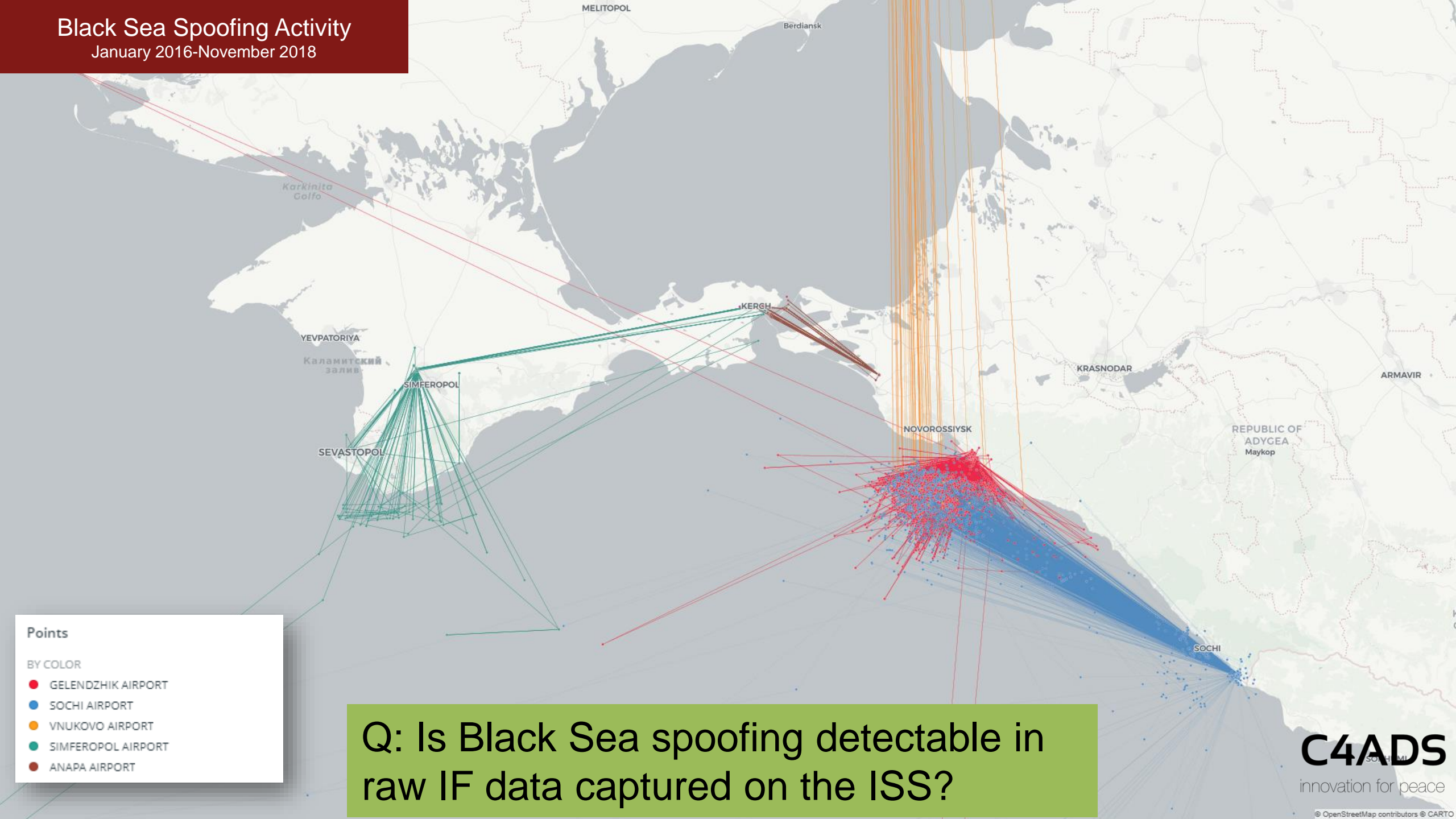
January 2016-November 2018

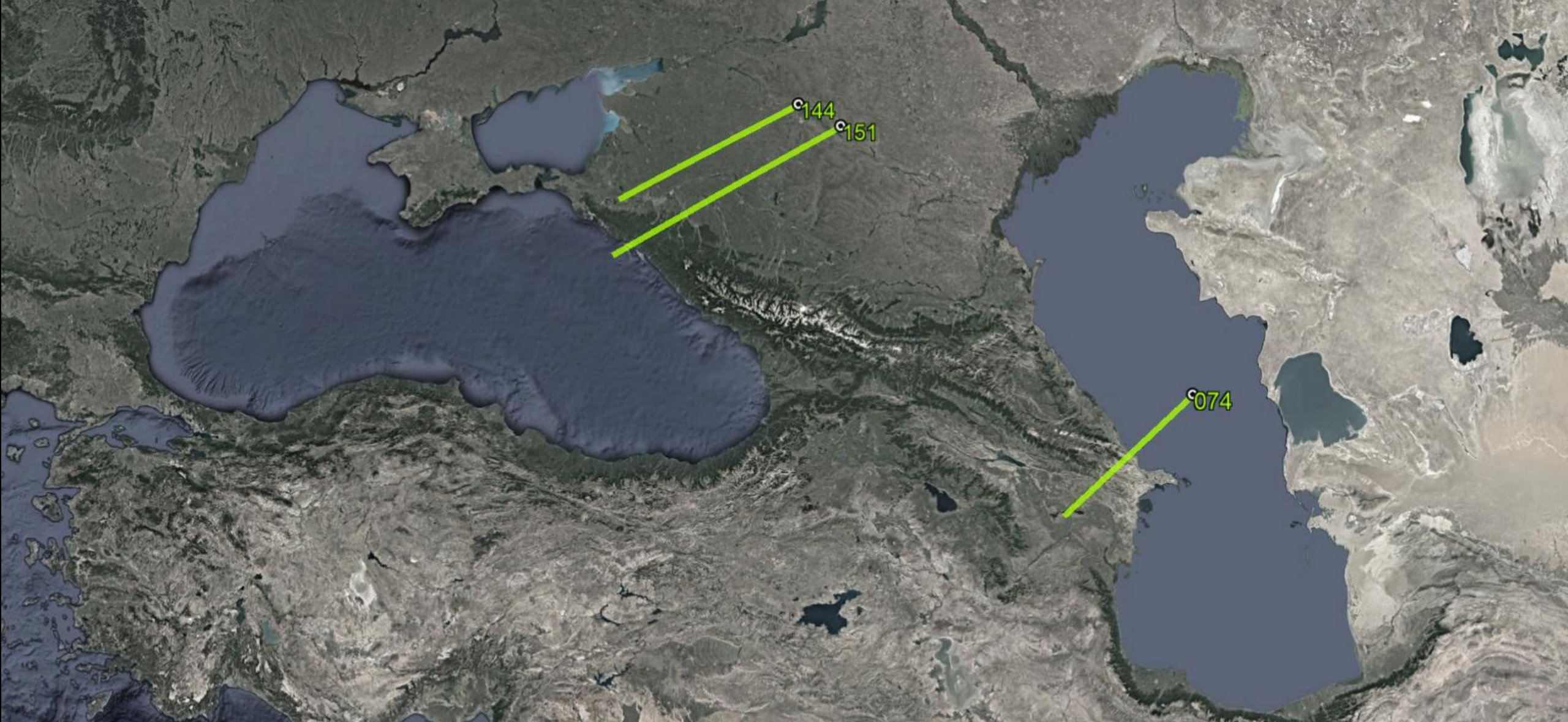
Points

BY COLOR

- GELENDZHIC AIRPORT
- SOCHI AIRPORT
- VNUKOVO AIRPORT
- SIMFEROPOL AIRPORT
- ANAPA AIRPORT

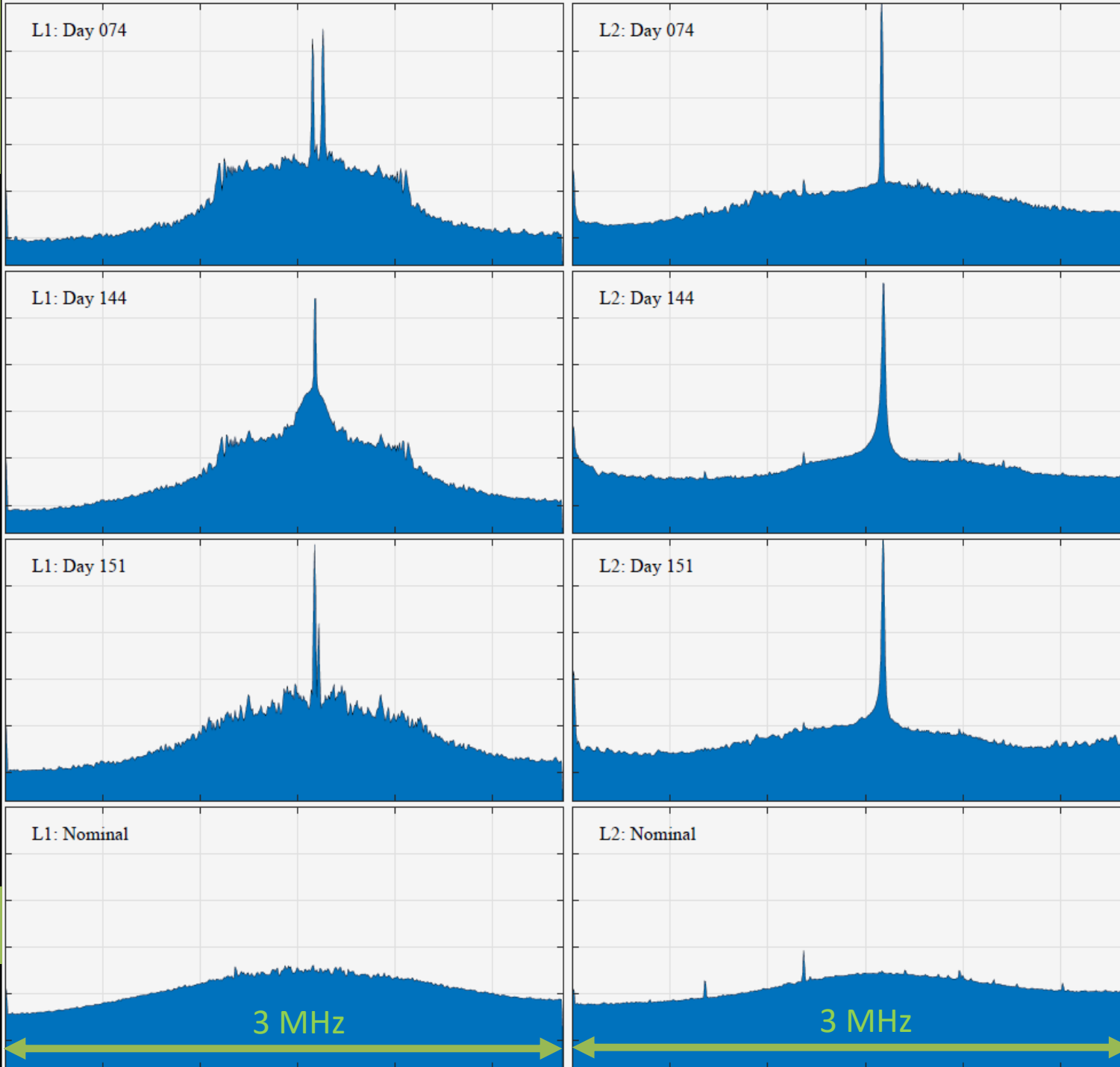
Q: Is Black Sea spoofing detectable in raw IF data captured on the ISS?





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

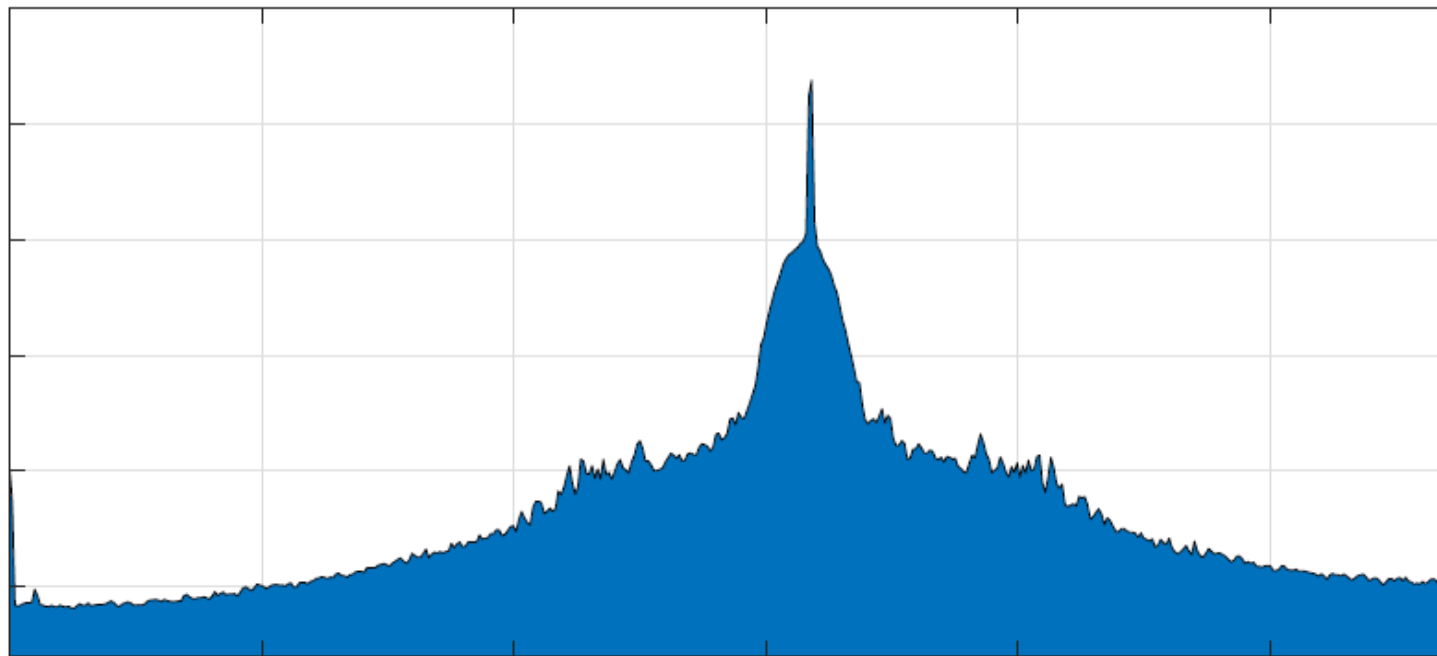
Power Spectra



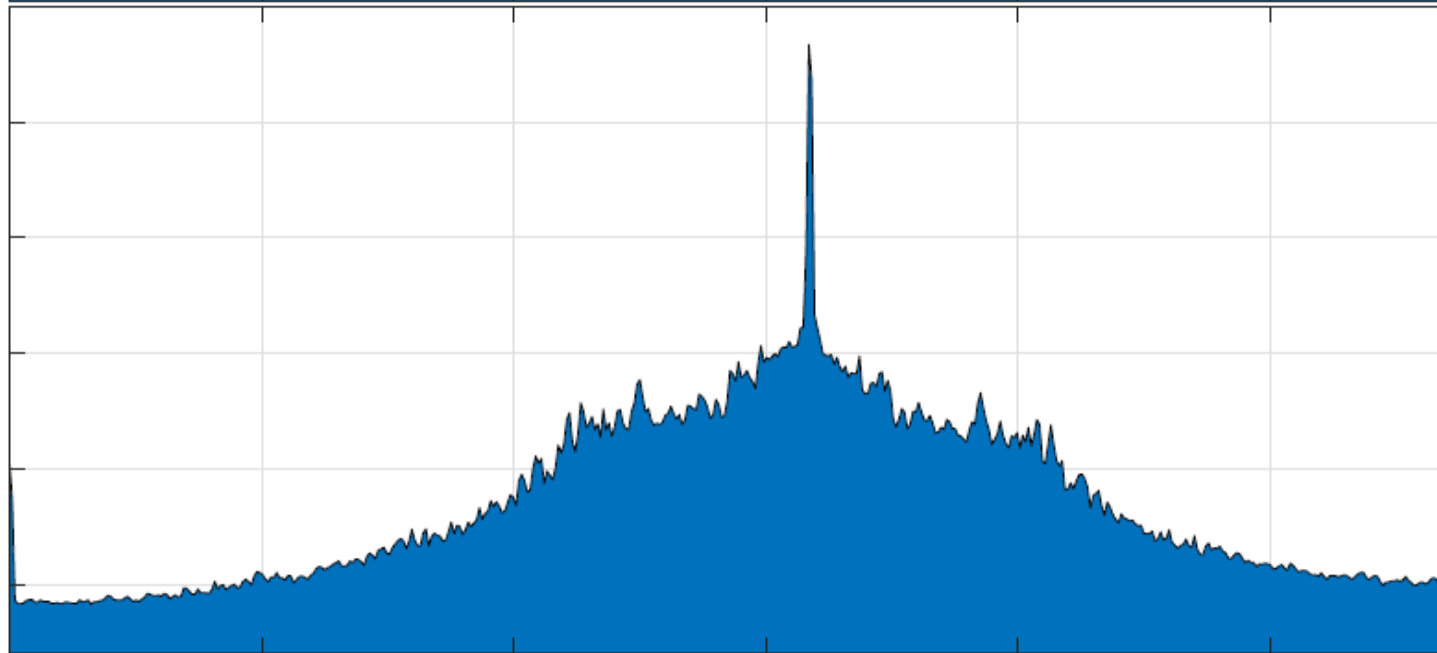
L1: 1575.42 MHz

L2: 1227.6 MHz

Maximum



Minimum



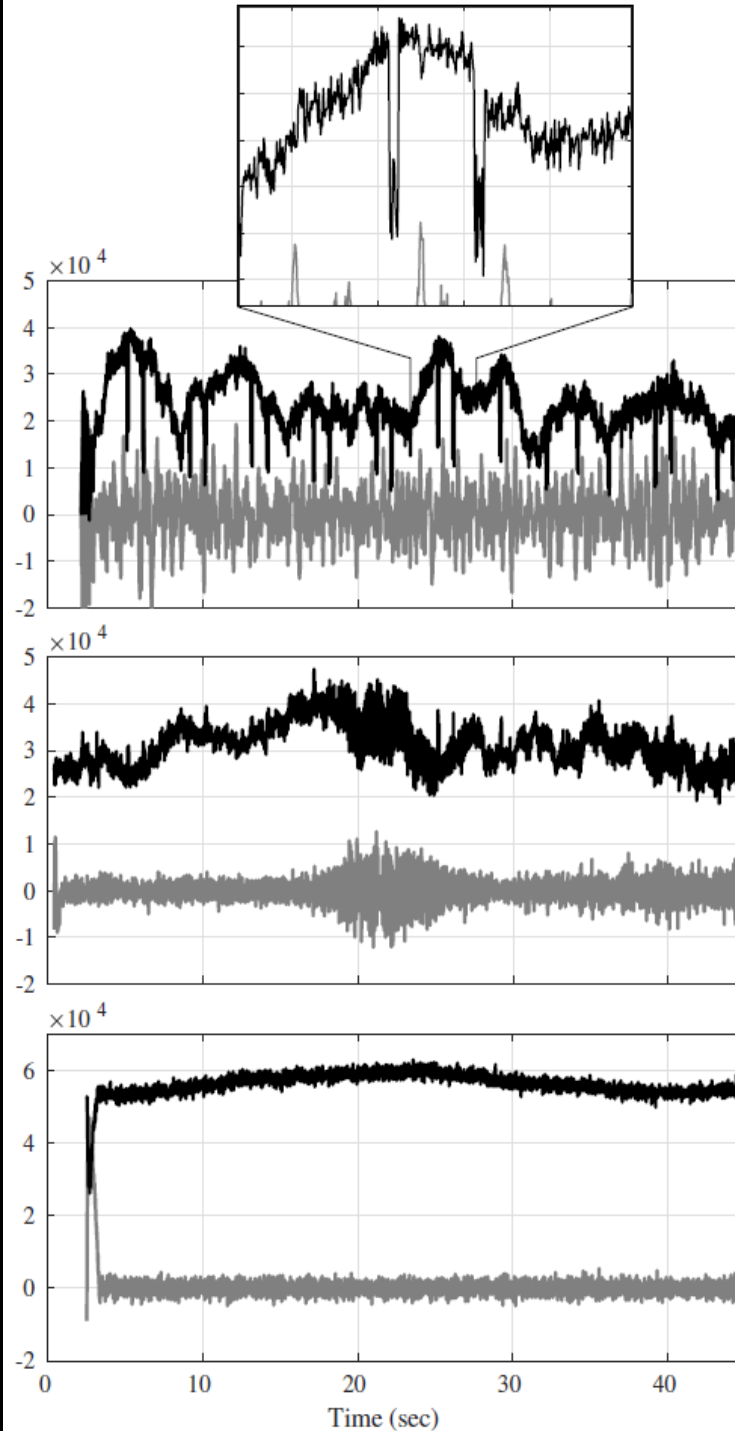
250 kHz rounded prominence at L1 waxes and wanes with an approximately 5 sec. period

Data-Wiped 100-Hz IQ accumulations

False signal

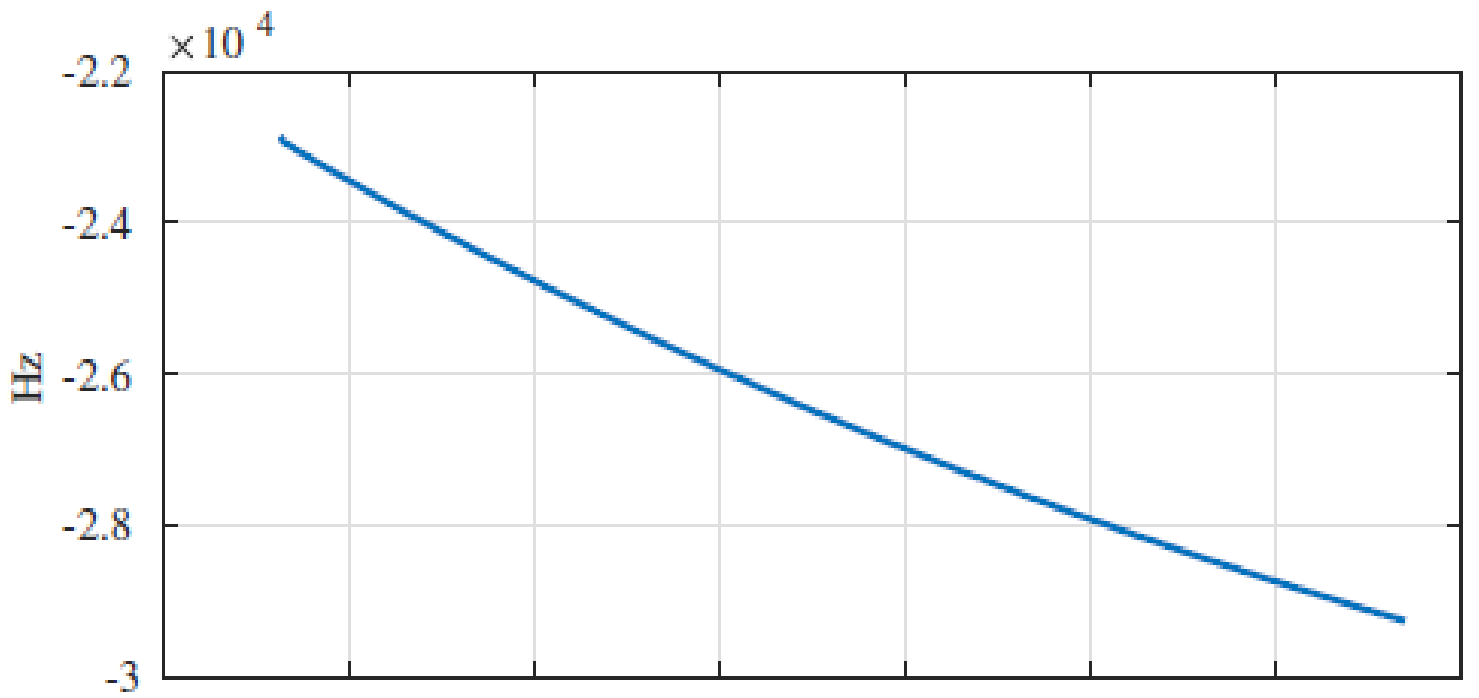
Authentic signal
in interference

Authentic signal
under clean
conditions

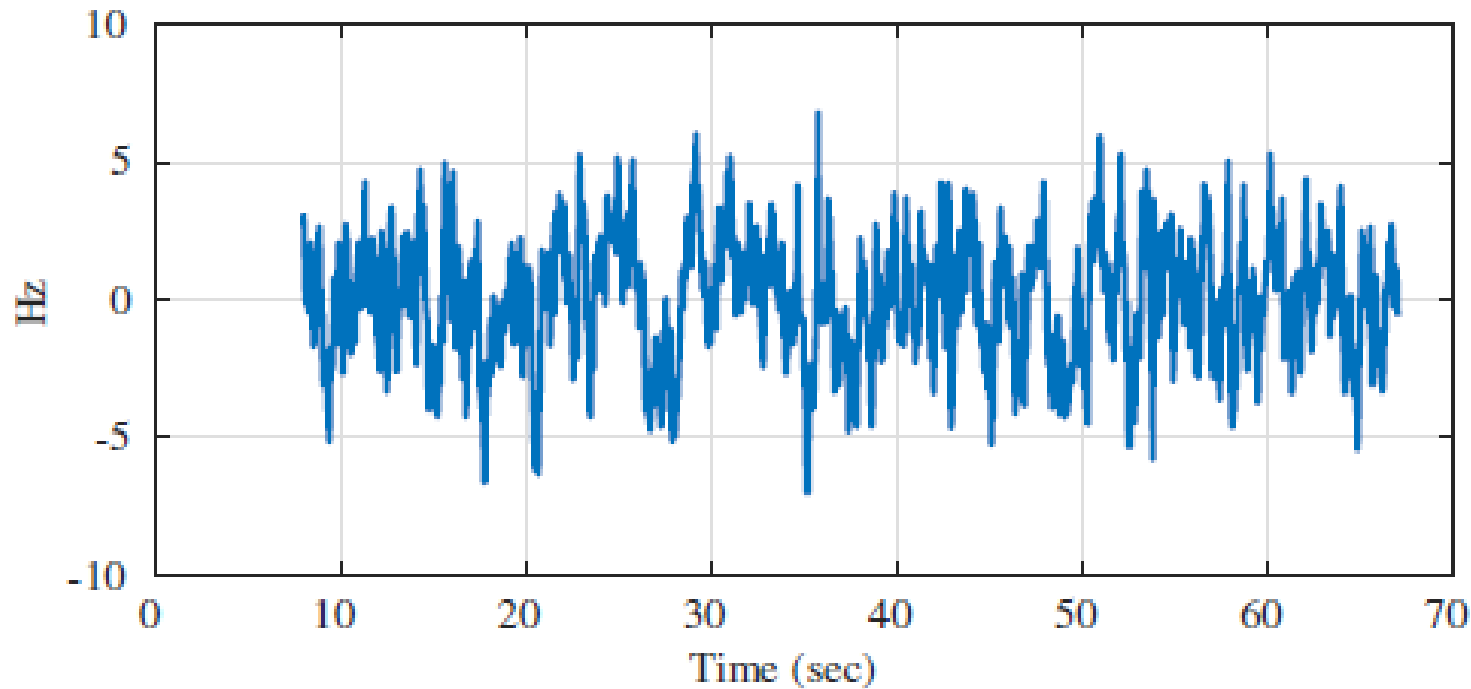


Unexplained
fading

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



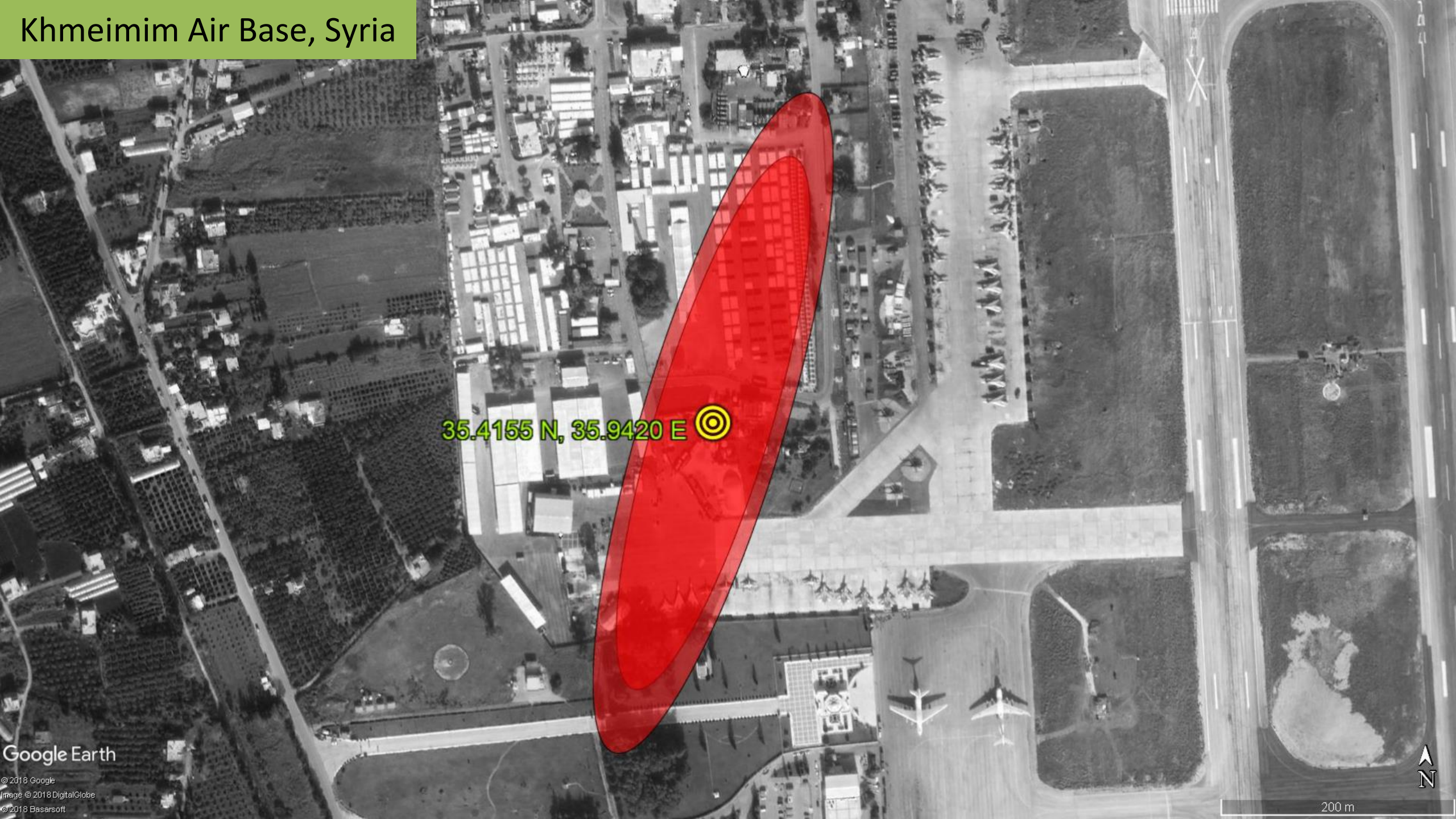
Post-fit residuals of
Doppler time history
assuming estimated
transmitter location
and clock rate offset



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

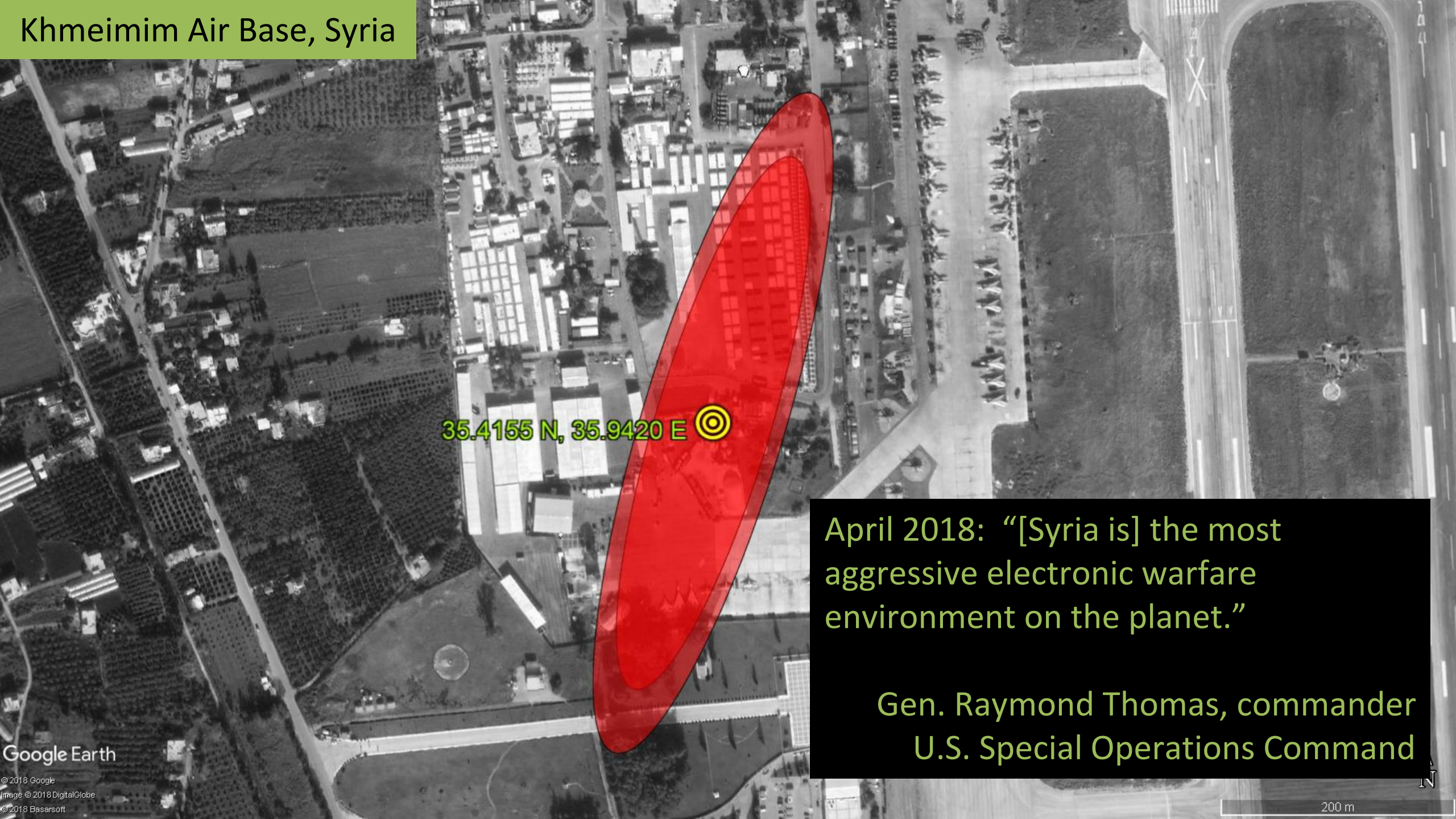



Khmeimim Air Base, Syria



35.4155 N, 35.9420 E

Khmeimim Air Base, Syria

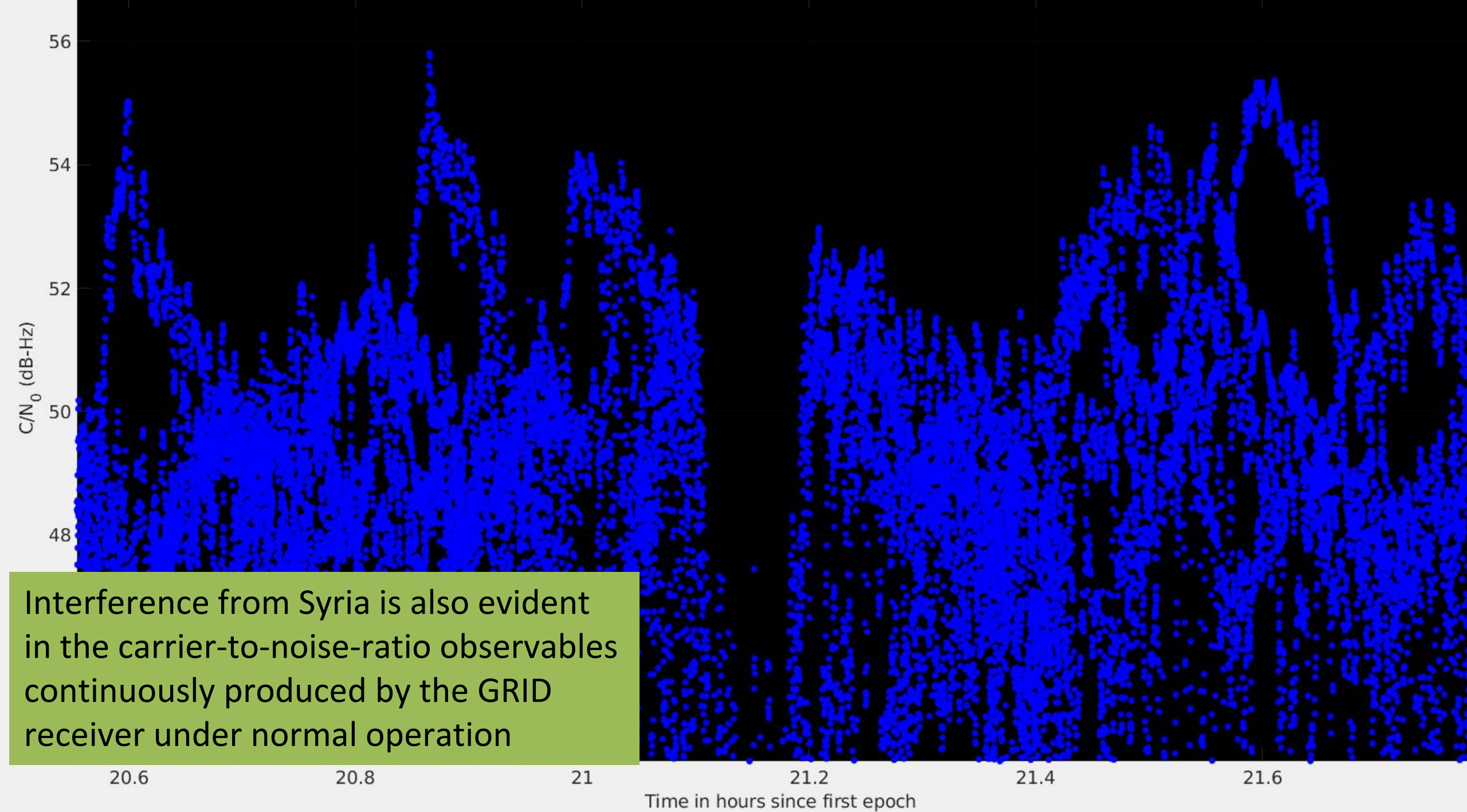


35.4155 N, 35.9420 E 

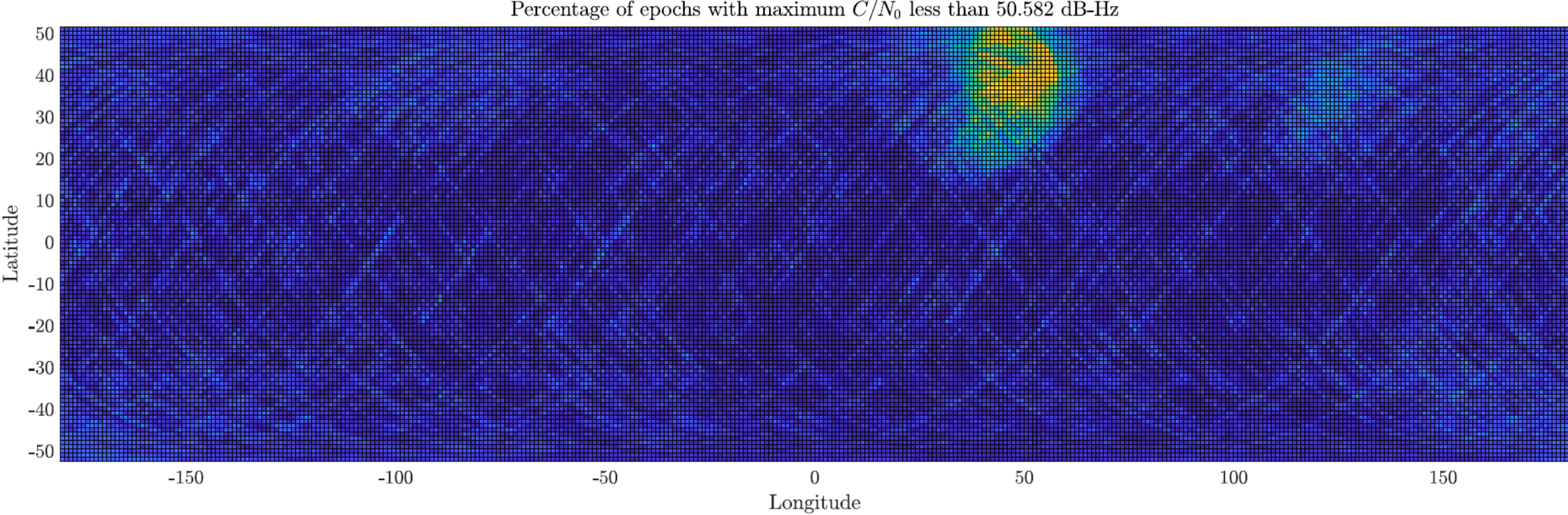
April 2018: “[Syria is] the most aggressive electronic warfare environment on the planet.”

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





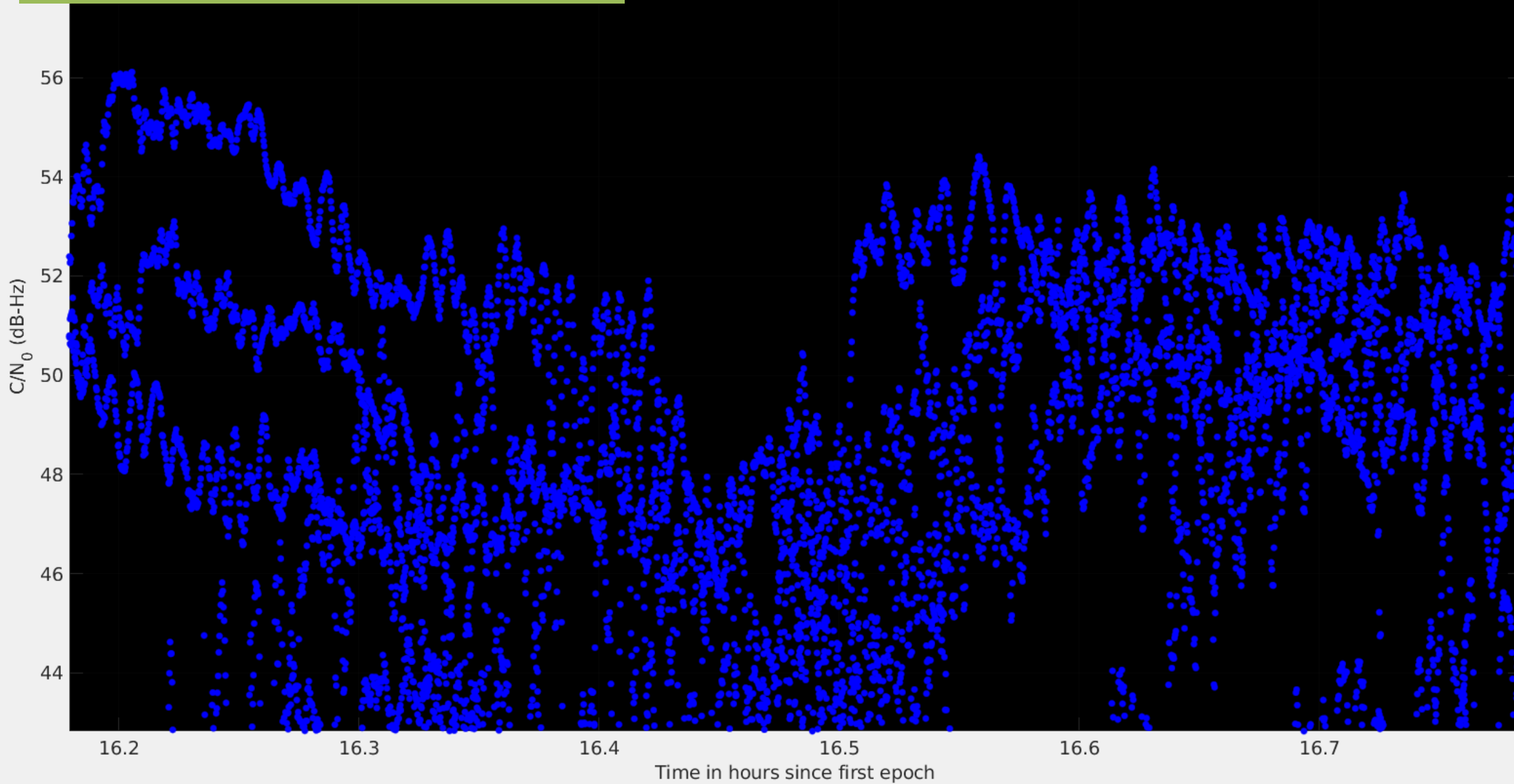
Interference from Syria is also evident in the carrier-to-noise-ratio observables continuously produced by the GRID receiver under normal operation



Heat map based on standard 1-Hz C/N_0 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



GPS L1 CA PRIMARY

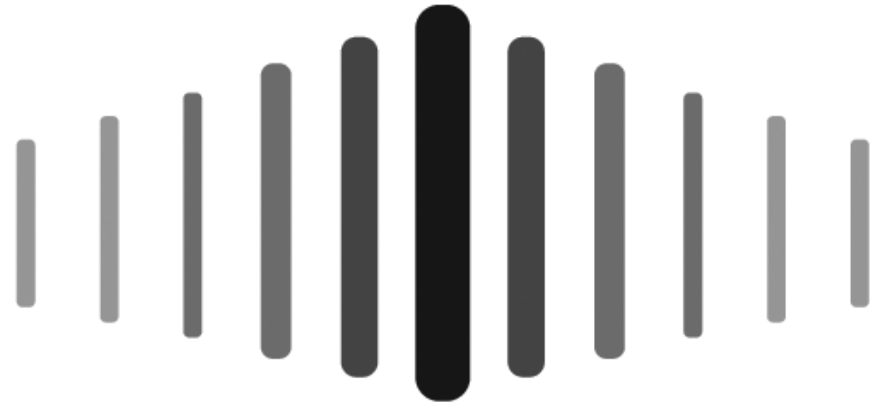
1	19u	-29228.2	-0.0	0.0	39.3	359.4	-75.1	5*
2	5u	-29228.2	-0.0	0.0	40.2	54.9	-38.4	5*
3	12u	-29228.7	-0.0	0.0	41.3	107.6	-47.8	5*
4	17u	-29226.3	-0.0	0.0	42.9	341.0	-59.1	5*
5	2u	-29227.7	-0.0	0.0	42.5	112.4	-58.6	5*
6	1u	-29226.9	-0.0	0.0	40.2	281.5	-17.5	5*
7	4	-31420.0	2097925.9	23905339.5	42.1	196.6	-4.0	6
8	16	-40379.6	2650169.5	21204591.2	40.5	220.0	10.2	6
9	18	-25577.3	1688476.6	21204591.2	40.5	220.0	10.2	6
10	22	-34506.5	2316331.2	21204591.2	40.5	220.0	10.2	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

“Coded” jamming via authentic spreading codes

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