Resilient and Robust PNT

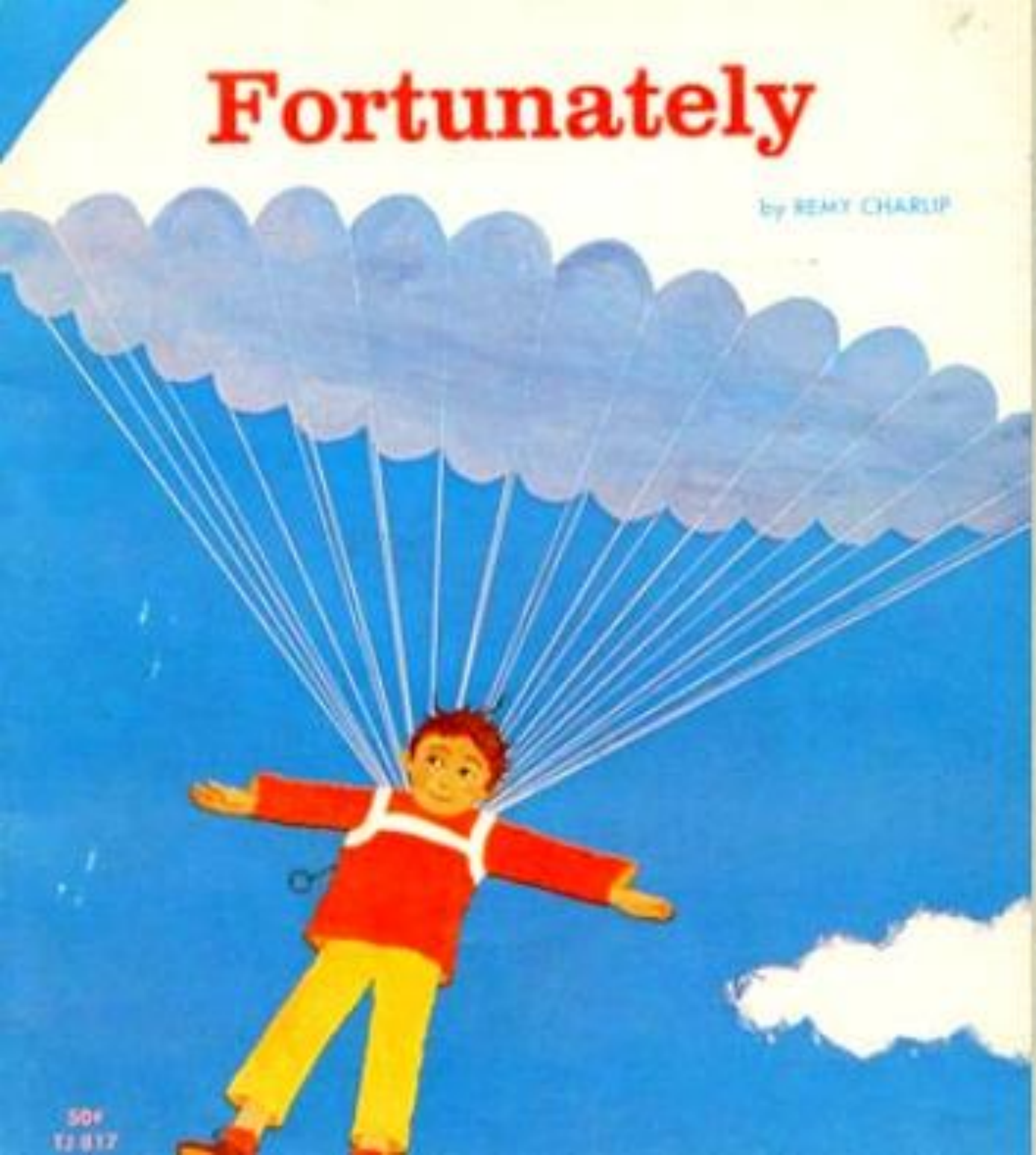
Todd Humphreys
With input from Peter Iannucci, Matthew Murrian, and Lakshay Narula
The University of Texas at Austin Radionavigation Lab

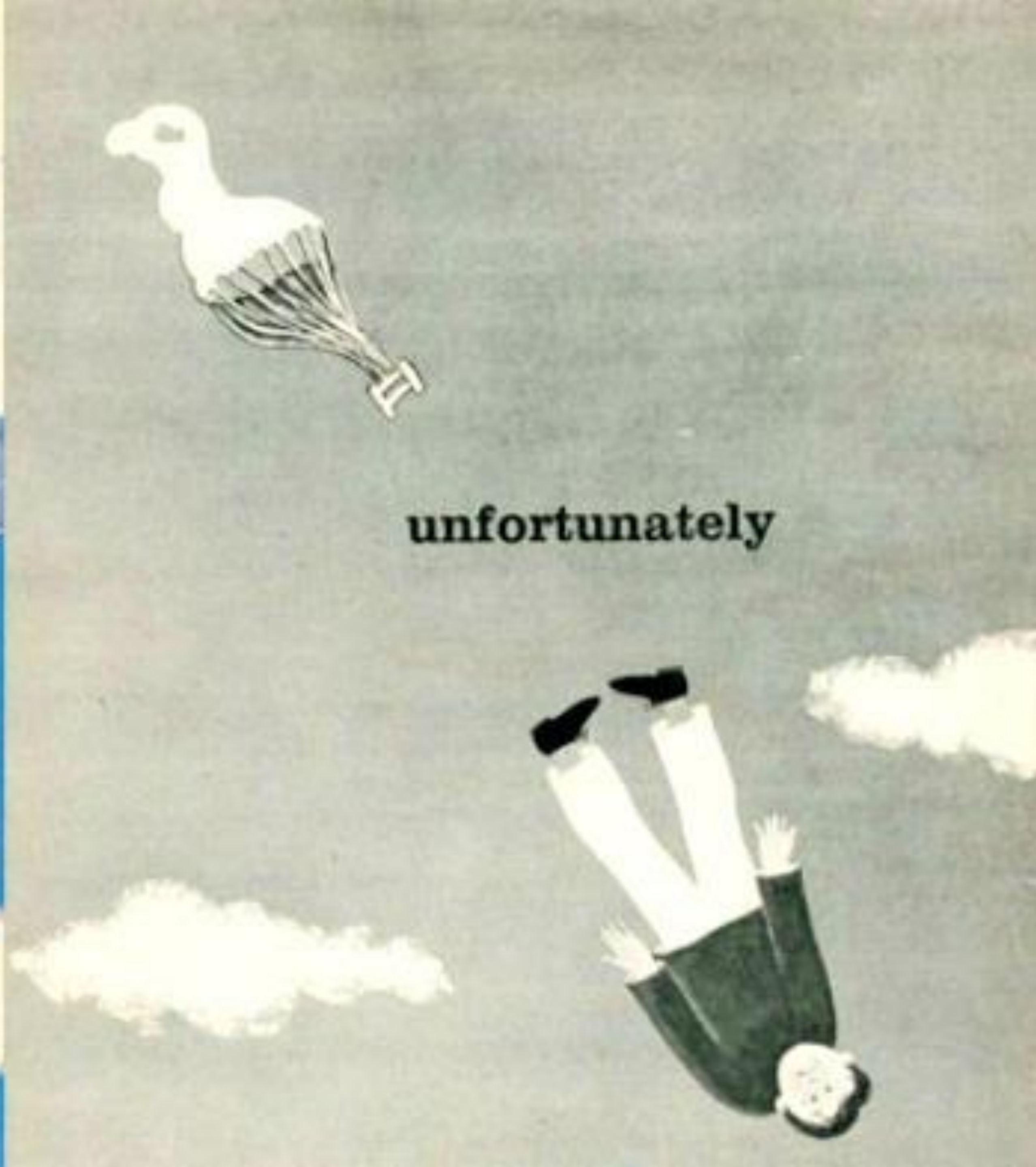
WNCG

THE UNIVERSITY OF TEXAS AT AUSTIN
RADIONAVIGATION LABORATORY

JNC Tutorial | August 24, 2021

All material in this presentation is drawn from the open literature. References are provided within and at the end of the presentation.


Fortunately
by REMY CHARLIP


unfortunately

4 billion GNSS devices in use globally

GSA 2015 market report

Core global revenue due to GNSS: $76B

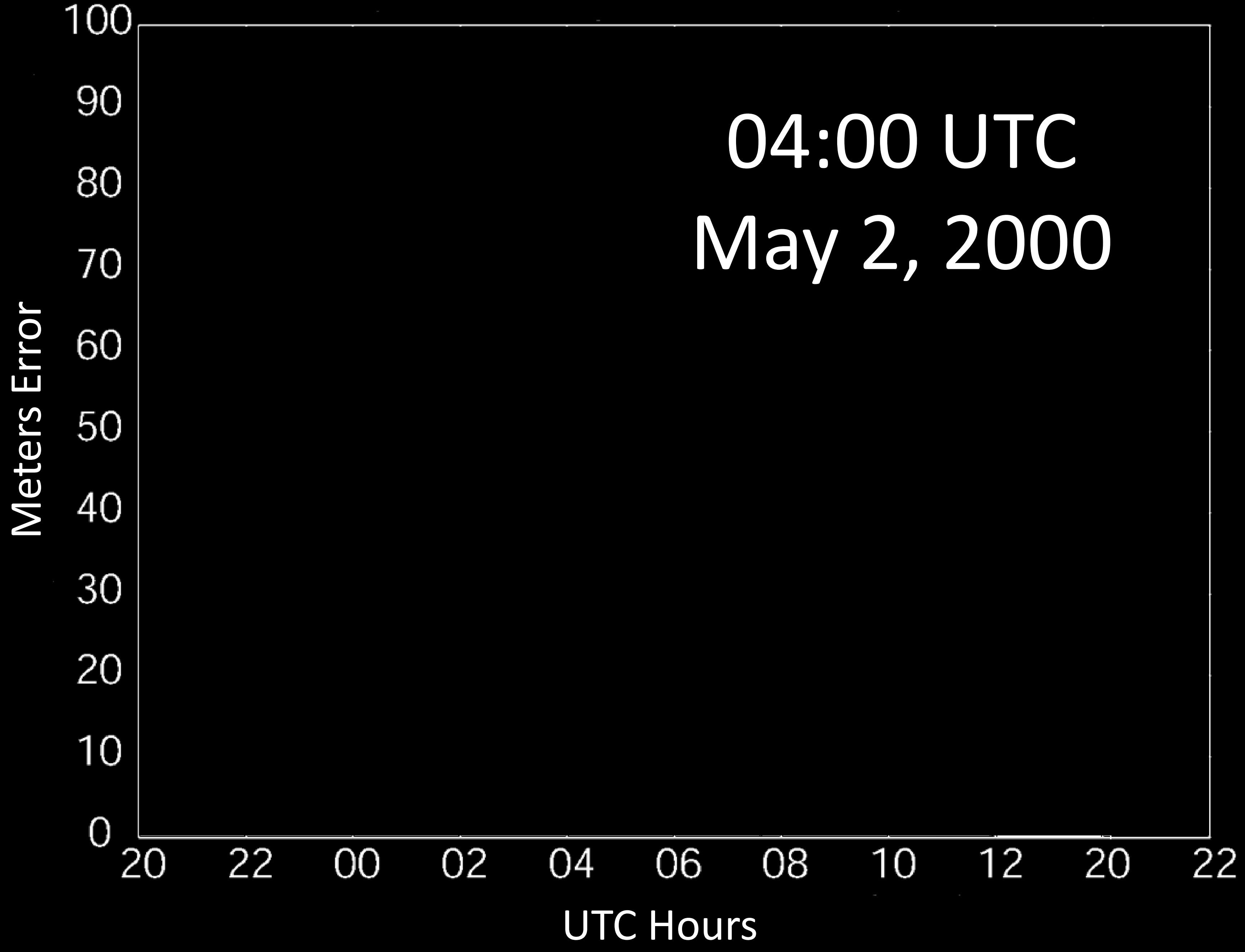
GSA 2015 market report

Enabled global revenue due to GNSS: $278B

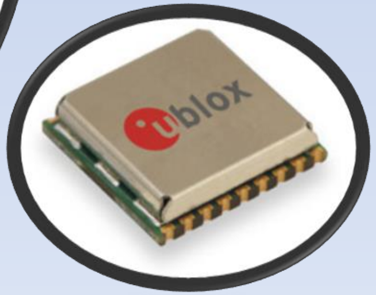
GSA 2015 market report

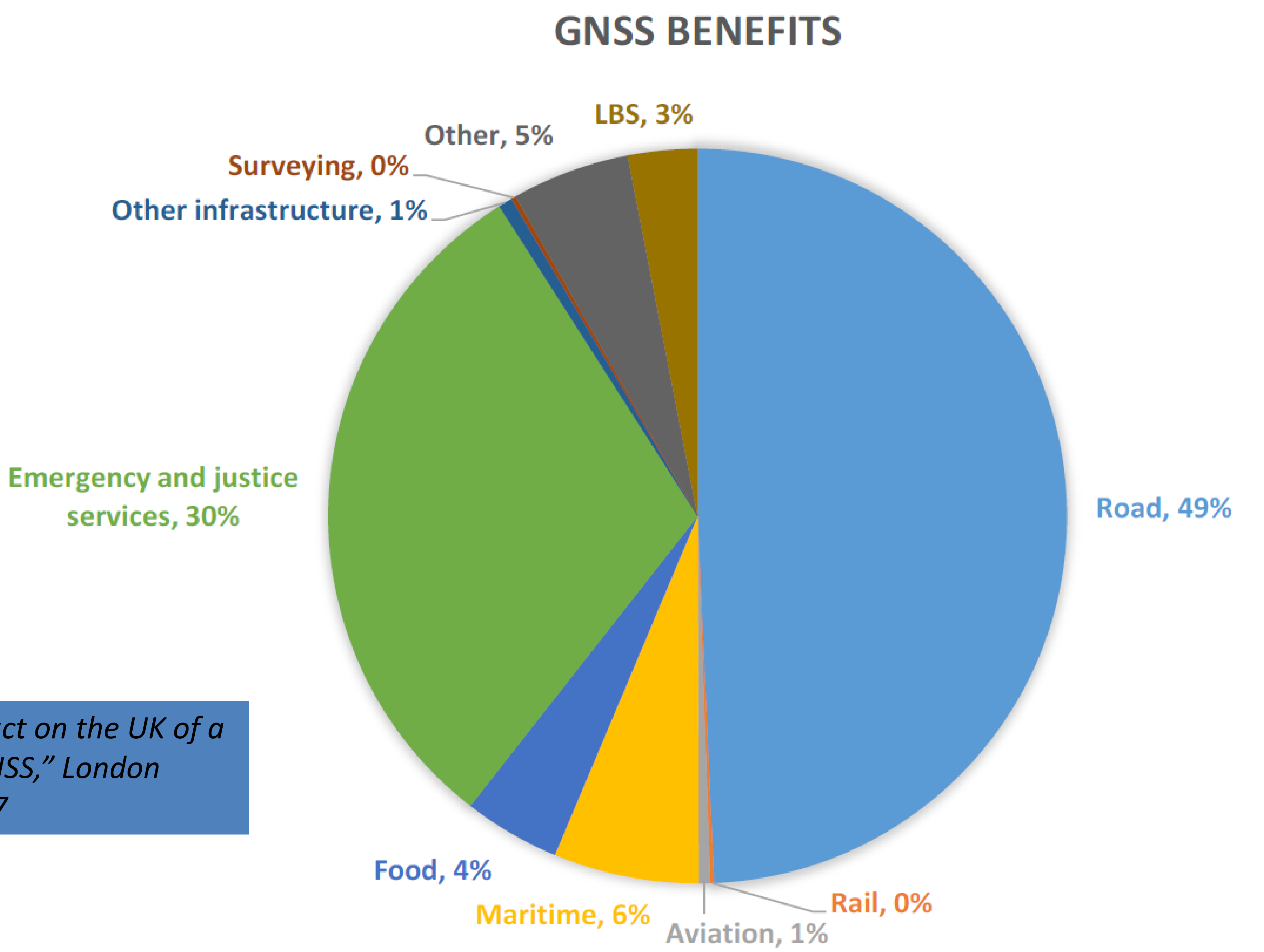
Economic cost to UK of 5-day GNSS outage: $7.2B

"Economic Impact on the UK of a disruption to GNSS," London Economics, 2017


04:00 UTC
May 2, 2000
Meters Error
100
90
80
70
60
50
40
30
20
10
0
20
22
00
02
04
06
08
10
12
20
22
UTC Hours


ASHTECH
GPS RECEIVER XII
NO WEST SOUTH MENU NORTH EAST YES
0 1 2 3 4 5 6 7 8 9

GPSMAP 64
GARMIN
IN OUT
FIND PAGE
MARK MENU
QUIT ENTER

ublox

"Economic Impact on the UK of a disruption to GNSS," London Economics, 2017

Q: Will GNSS remain the pre-eminent worldwide source for positioning, navigation, and timing (PNT)?

A: Unfortunately, serious GNSS vulnerabilities need addressing; these may be unfixable.

Two schools of thought:

(1) Fix GNSS

(2) Seek stand-alone alternative sources of PNT

PTA

Protect
Toughen
Augment

APNT

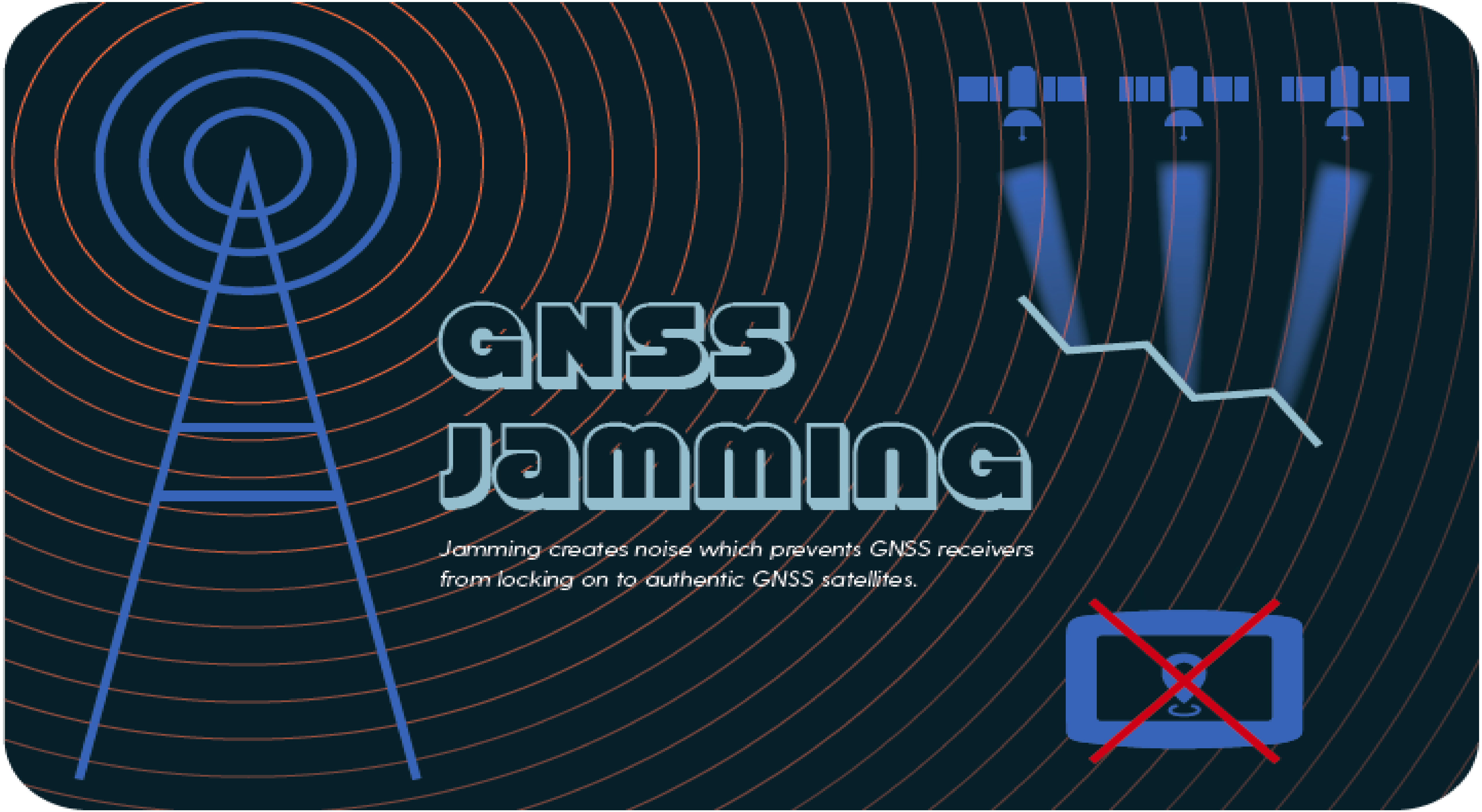
Alternative
Positioning
Navigation
Timing

“Needed: About 35 dB of additional receiver interference resistance.”

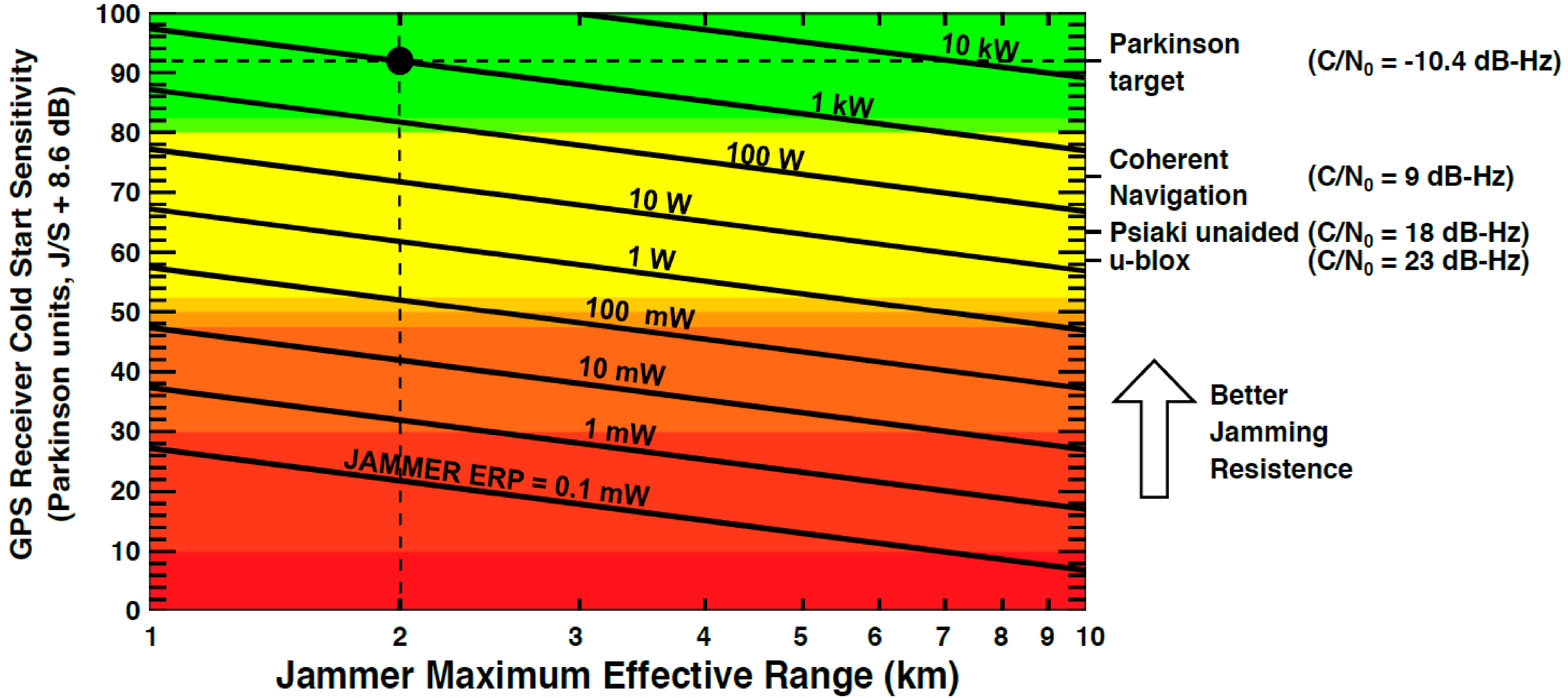
Bradford Parkinson, Architect of GPS, “Nibbles,” 2012

“… we’re looking beyond GPS … we need to find alternatives for military use that are more resilient and less vulnerable.”

Former Sec. Defense Ash Carter giving Drell Lecture at Stanford in 2015


GNSS
Jamming
Jamming creates noise which prevents GNSS receivers from locking on to authentic GNSS satellites.

1 kW wideband jammer can deny service to the best COTS GNSS receivers over a ~200 km (line-of-sight) effective range



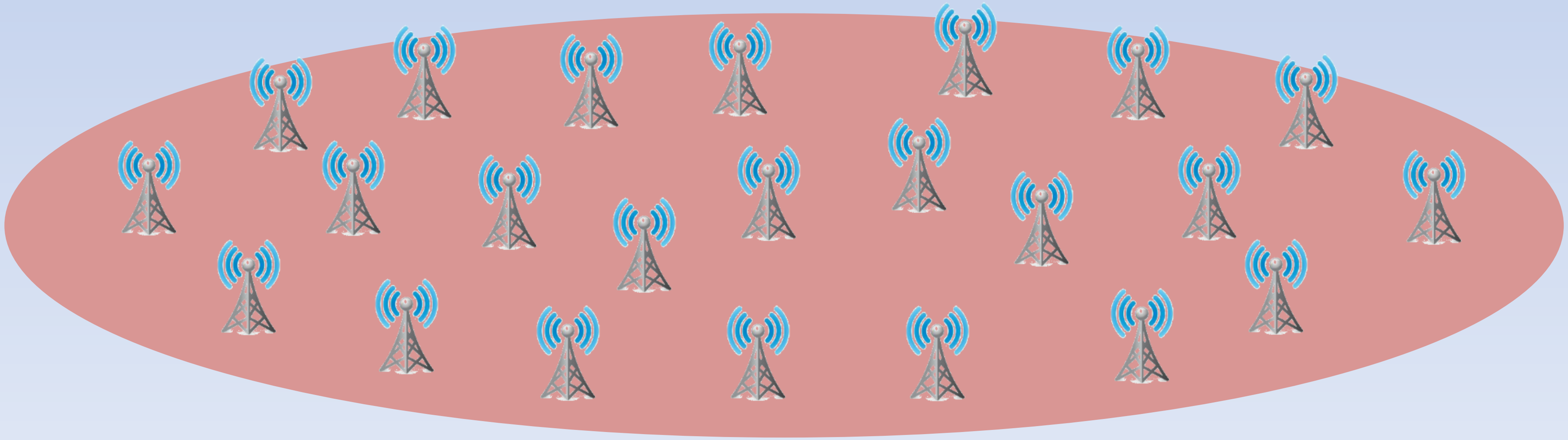
PTA: By (1) deep coupling with inertial sensors, and (2) multi-element antennas we can toughen GNSS receivers enough to withstand 1 kW wideband Gaussian jammer at a distance of 2 km.

Deploying full combination of best current technology
could shrink effective range to 2 km.
Moreover, the jammer itself becomes a counterstrike target.

But cost asymmetry favors the jammer:

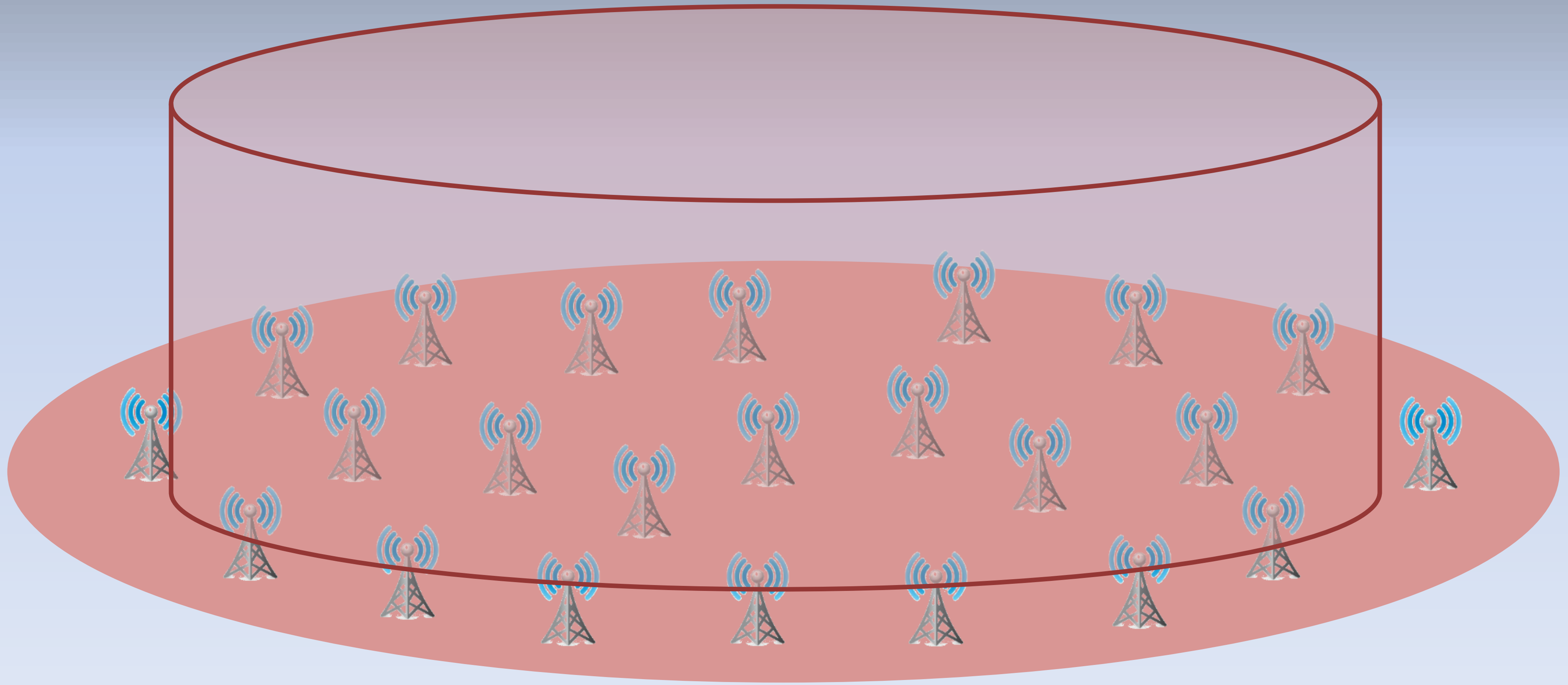
1 kW jammer cost: ~$200

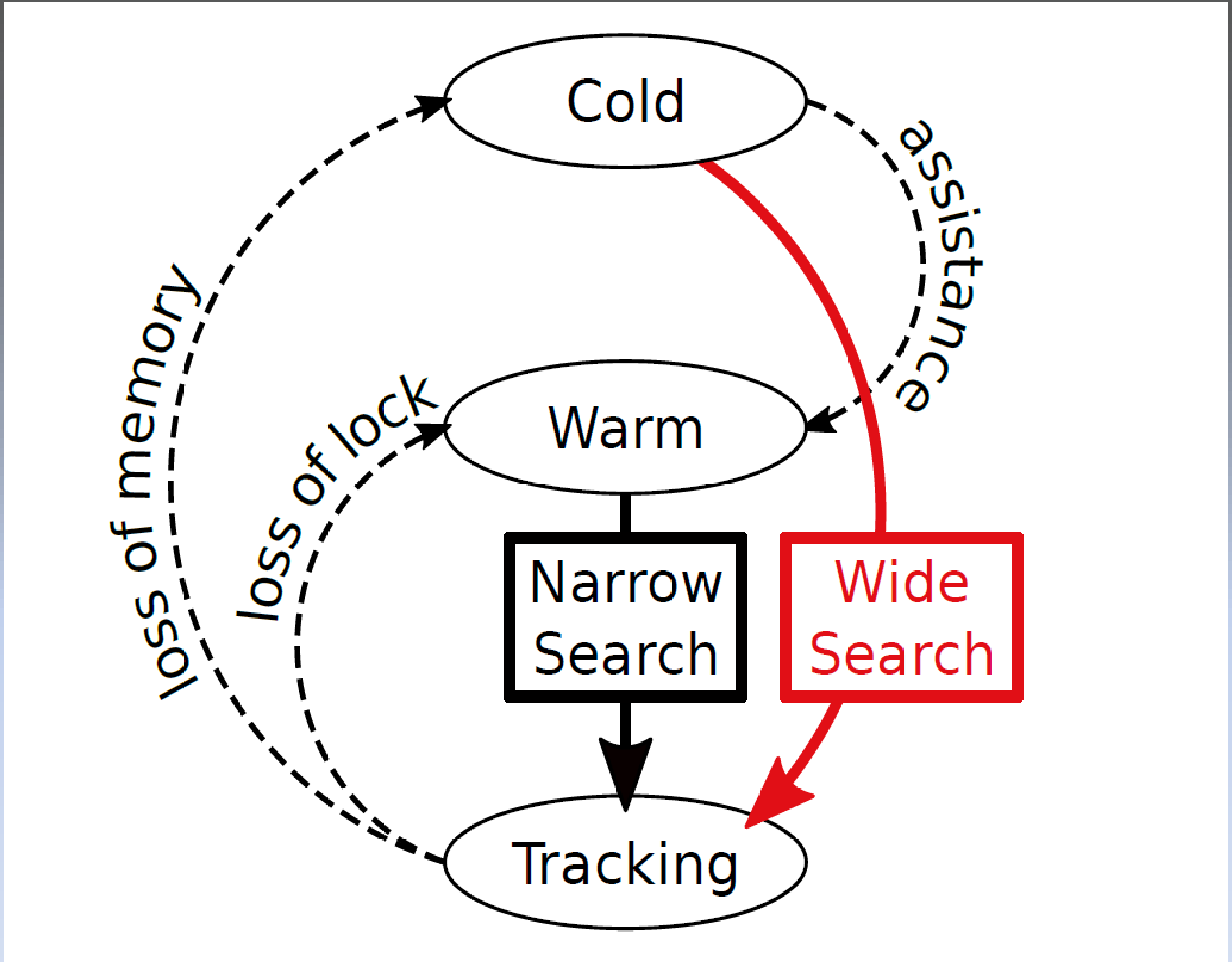
Cost for enough jammers to deny service in 200-km-radius zone: ~$2 M



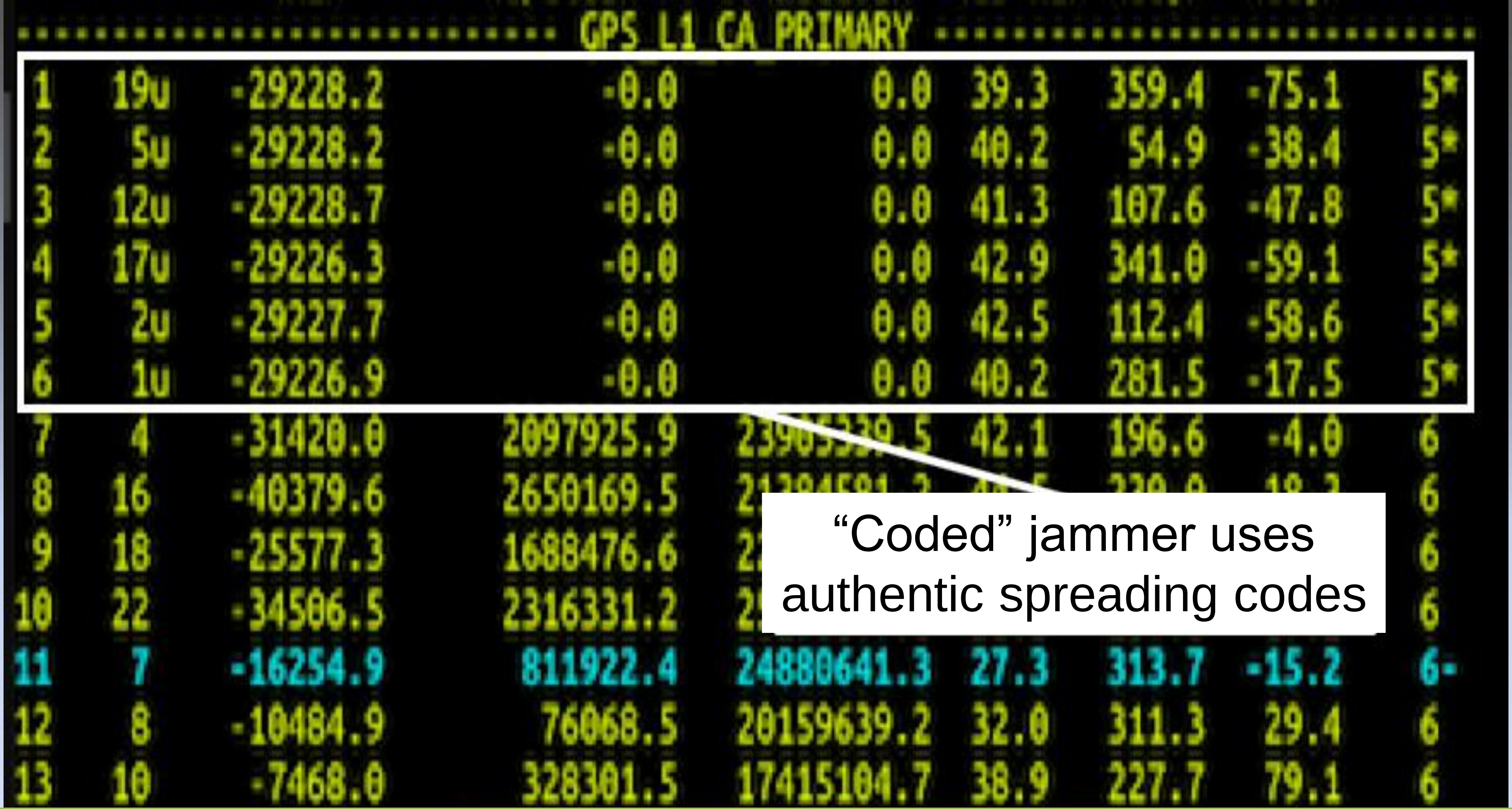
But cost asymmetry favors the jammer:

- 1 kW jammer cost: ~$200
- Cost for enough jammers to deny service in 200-km-radius zone: ~$2 M
- Jamming power now remains constant with altitude



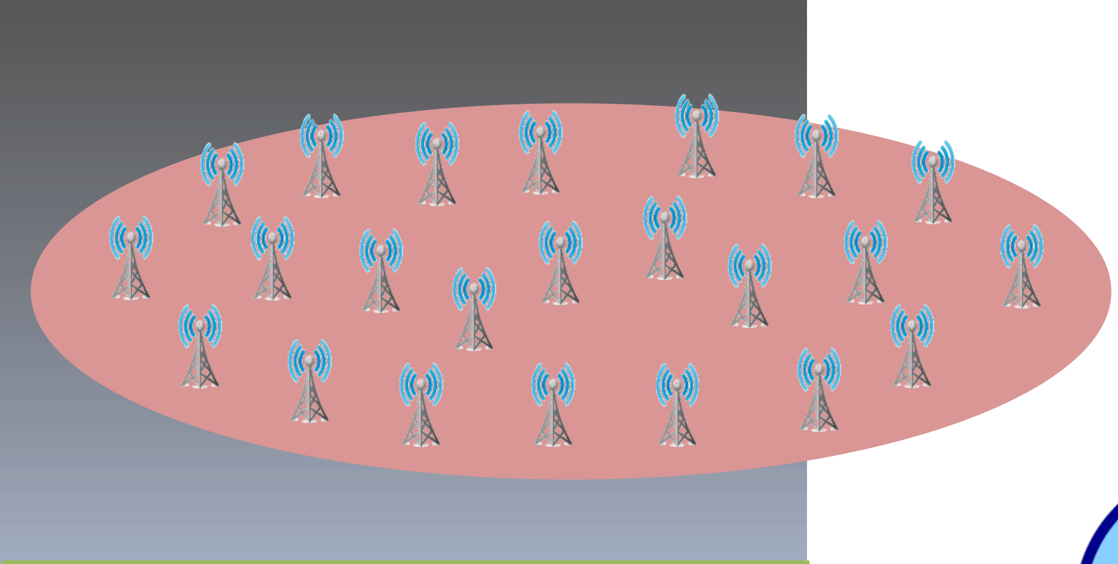


What is more, immunity to J/S = 84 dB jamming environment almost certainly requires warm start for encrypted (non-repeating) wideband codes such as M-code: side channel must provide approximate time and location.

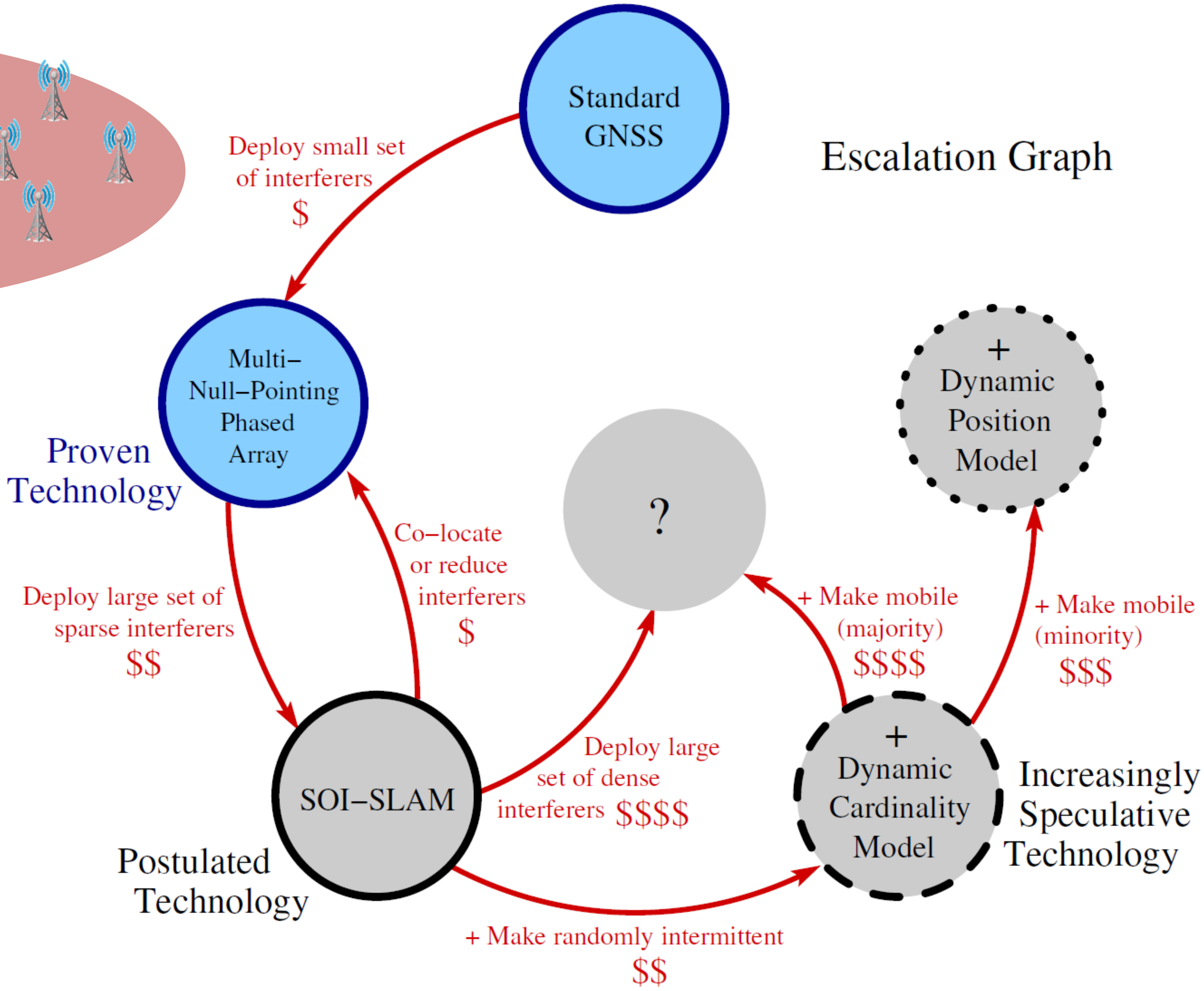


A coded jammer (or meacon) is more potent than uncorrelated wideband jammer: Each coded signal produces a correlation peak competitor that must be distinguished from authentic peak.

Upshot: even 35 dB of additional interference resistance (expensive!) would not prevent a determined adversary from cost-effectively denying GNSS over an area the size of Colorado.

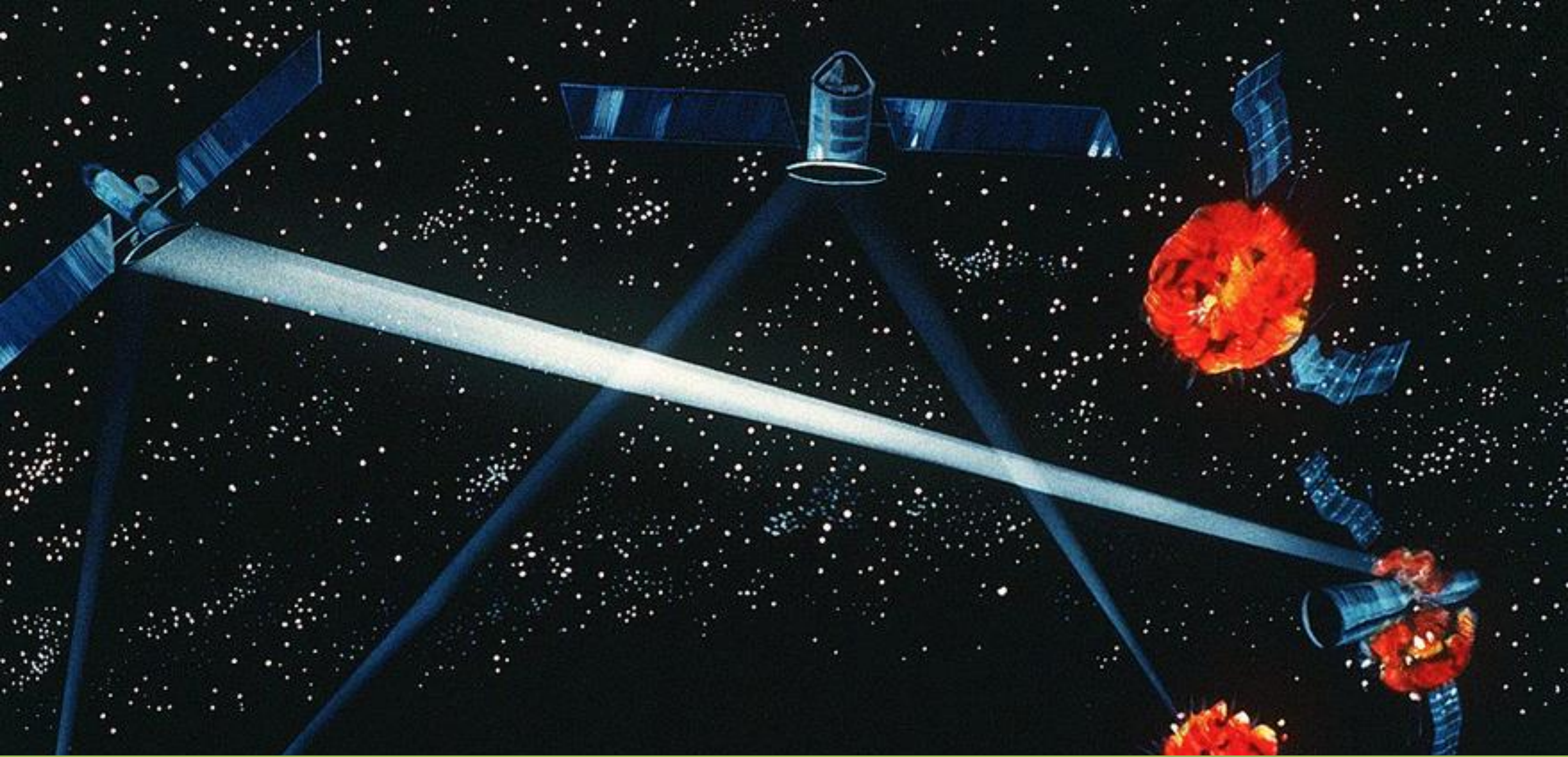


The “fortunately, unfortunately” game can be played with distributed jamming technology: the defender can use the jamming sources as beacons in a “Signal of Opportunity from Interference (SOI) Simultaneous Localization and Mapping (SLAM)” framework.



Q: Could directed energy weapons damage GNSS satellites?

Directed energy: <u>current technology</u> could jam but not damage: Recently-completed Chinese FAST radio telescope is largest in world: 300-meter diameter steerable aperture. If used to focus energy of a massive 466 MW magnetron, power flux at MEO would be only 20 Watts per square meter, less than 1/50 of solar irradiance.



Directed energy: <u>future technology</u> (e.g., space lasers) could damage GNSS satellites

“[An influential view within China] is that this next phase [of warfare] will be characterized by combining manipulations of “Big Data” and increasing autonomy/artificial intelligence, with directed energy weapons at the core.”

Fisher, R. D. "China’s Progress with Directed Energy Weapons." *International Assessment and Strategy Center, Washington, DC* (2017).

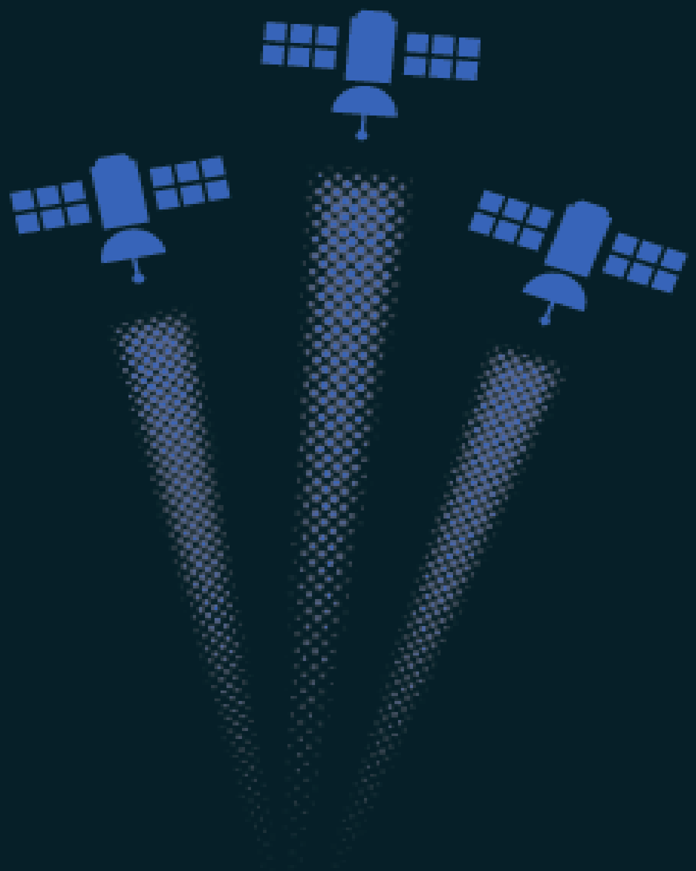
Q: Could direct-ascent kinetic ASAT weapons destroy GNSS satellites?

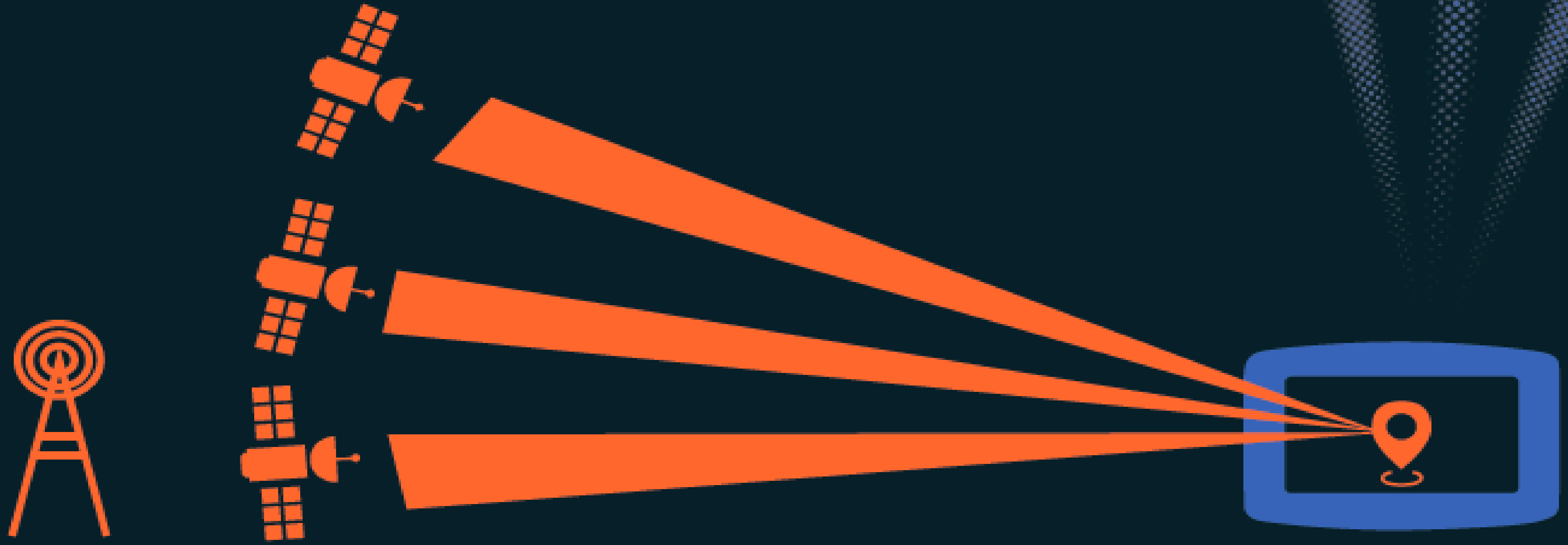
May 2013: Chinese launched experimental direct-ascent ASAT weapon that reached beyond GPS orbit.

Direct-ascent ASAT could destroy individual satellites, but it would be impractical to take out full GPS constellation.

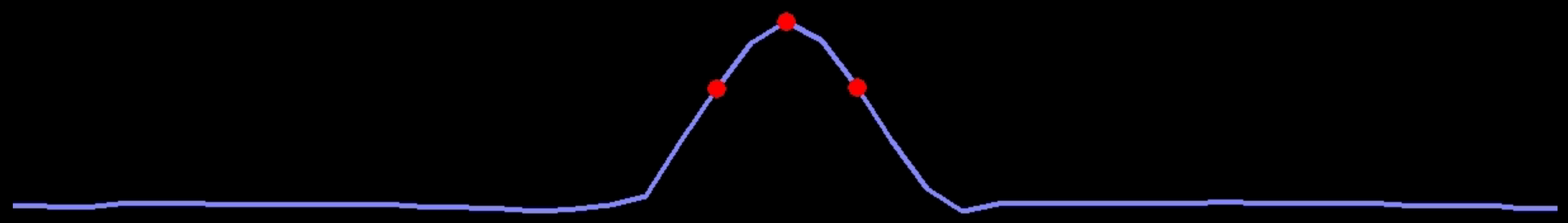
GNSS SPOOFING

Spoofing mimics authentic GNSS satellites to hijack GNSS receiver tracking loops.

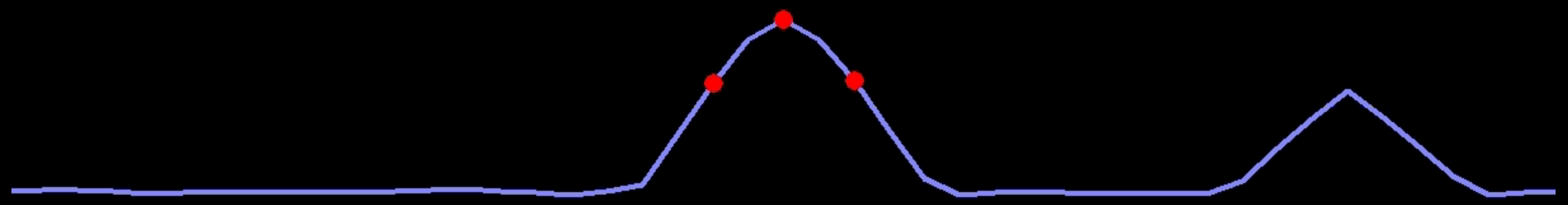




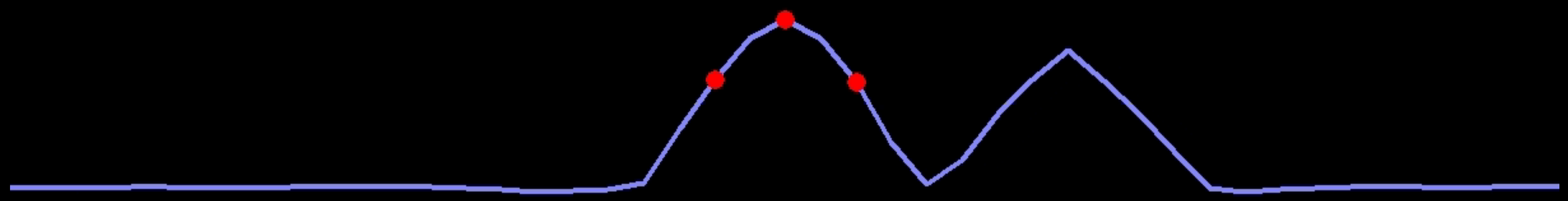
GPS Spoofer



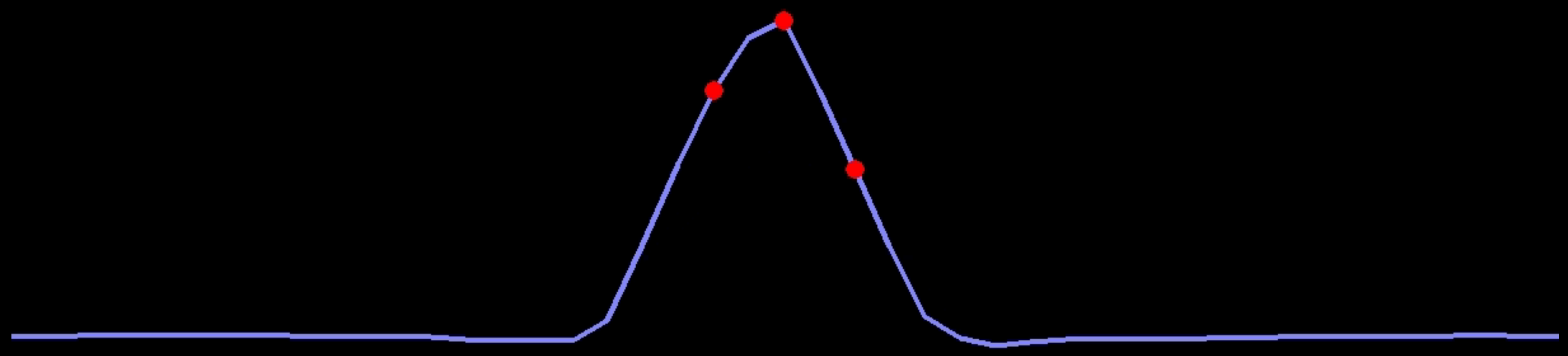
GPS Spoofer



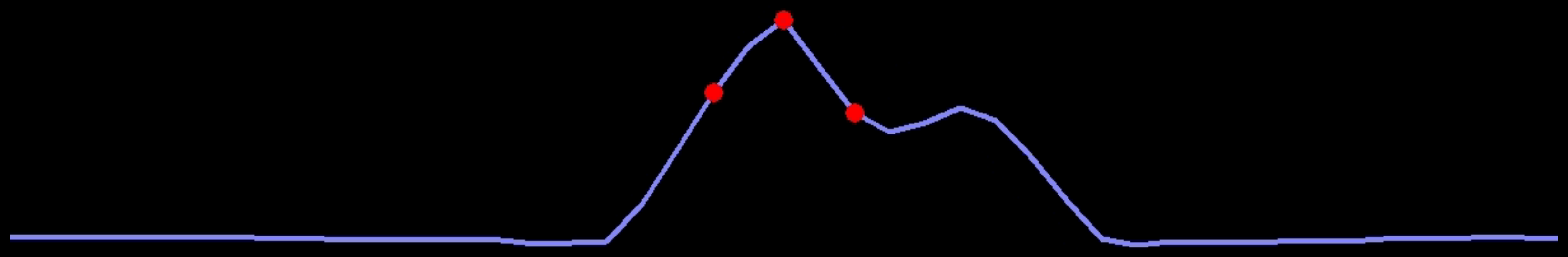
GPS Spoofer



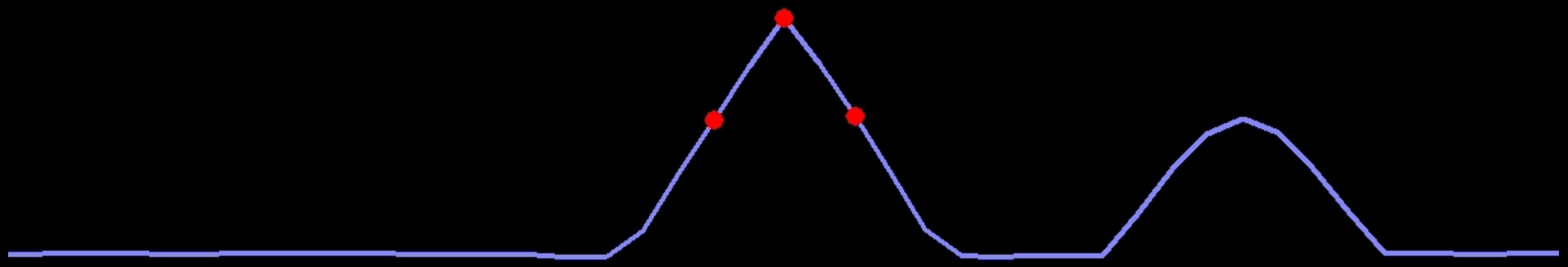
GPS Spoofer



GPS Spoofer



GPS Spoofer

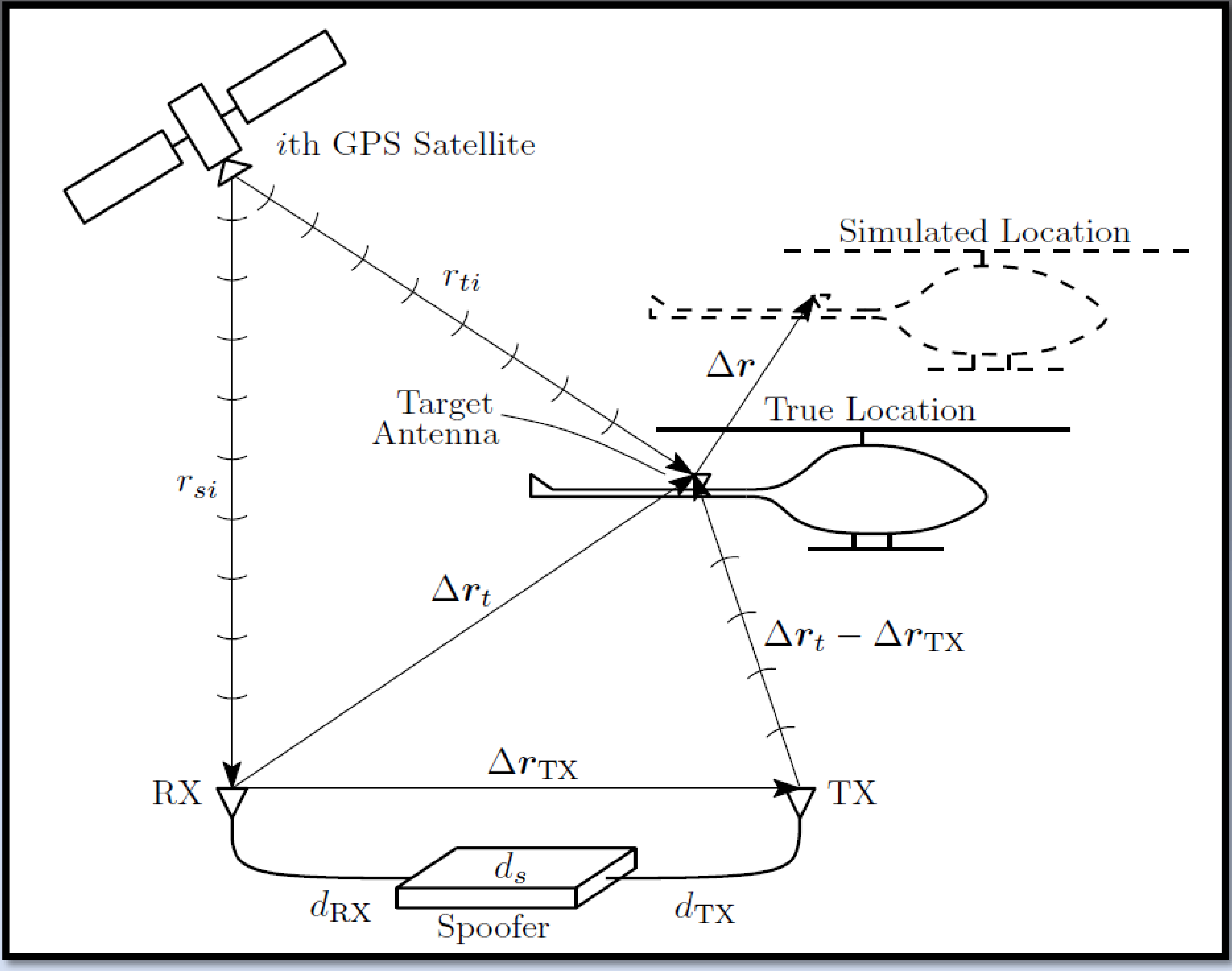


Q: Is the GNSS spoofing vulnerability only theoretical, or has it been proven by experiment?

Building the first publicly-acknowledged GPS spoofer, 2008

Humphreys, Todd E., et al. "Assessing the spoofing threat: Development of a portable GPS civilian spoofer." *Proceedings of the 21st International Technical Meeting of the Satellite Division of The Institute of Navigation (ION GNSS 2008)*. 2008.

First target: personal iPhone

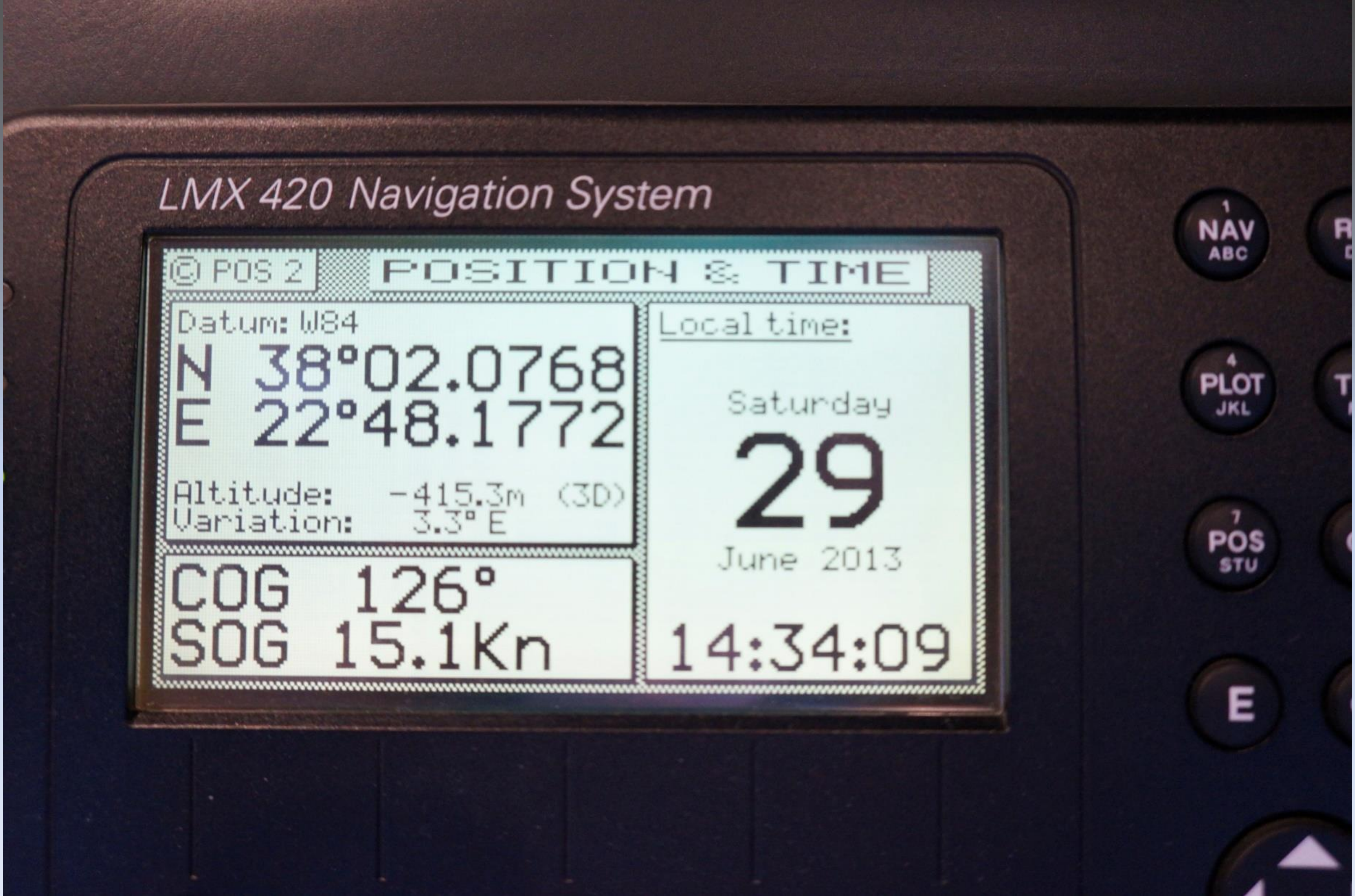


Could false GNSS signals cause UAV to believe it’s at the spoofer-simulated location, allowing full 3D hostile control of UAV?

$60k Hornet Mini's navigation system sensors:
civil GNSS + baro + IMU + magnetometer

Kerns, Andrew J., Daniel P. Shepard, Jahshan A. Bhatti, and Todd E. Humphreys. "Unmanned aircraft capture and control via GPS spoofing." *Journal of Field Robotics* 31, no. 4 (2014): 617-636.

White Rose of Drachs: 65-meter, $80M research laboratory in the Mediterranean


LMX 420 Navigation System
POS 2
POSITION & TIME
Datum: W84
N 38°02.0768
E 22°48.1772
Altitude: -415.3m (3D)
Variation: 3.3° E
COG 126°
SOG 15.1Kn
Local time:
Saturday
29
June 2013
14:34:09
NAV
ABC
PLOT
JKL
POS
STU
E

Bhatti, Jahshan, and Todd E. Humphreys. "Hostile control of ships via false GPS signals: Demonstration and detection." *NAVIGATION, Journal of the Institute of Navigation* 64.1 (2017): 51-66.

ubscribe for $1 a week. THE NEW YORKER Newsletter Sign In Subscribe

News Books & Culture Fiction & Poetry Humor & Cartoons Magazine Crossword Video Podcasts Archive Goings On

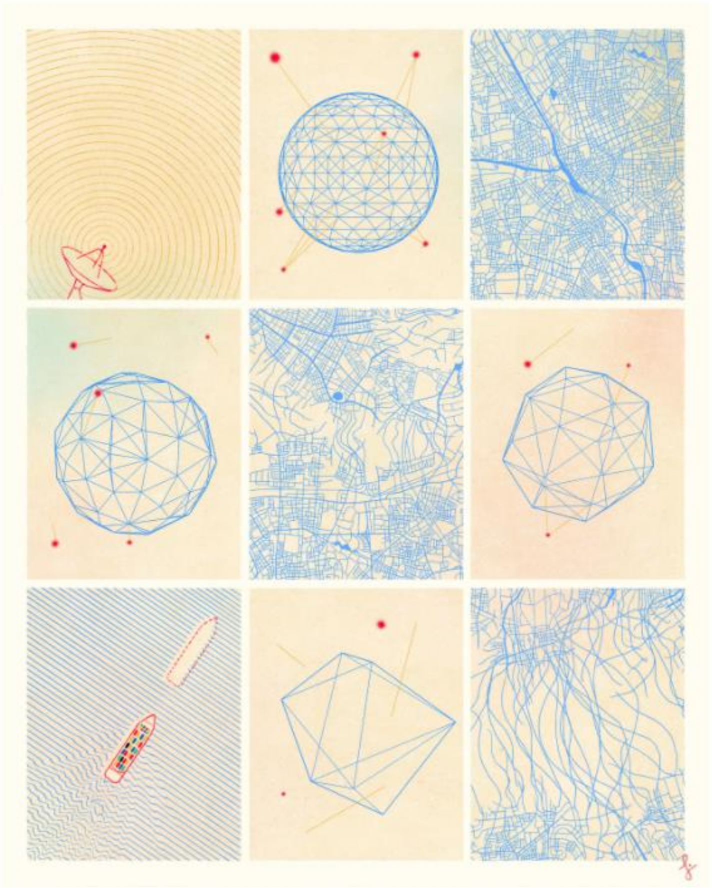
ANNALS OF TECHNOLOGY

HOW VULNERABLE IS G.P.S.?

An engineering professor has proved—and exploited—its vulnerabilities.

By Greg Milner

August 6, 2020



Profile of UT Radionavigation Lab’s research in GNSS vulnerabilities over past decade: *The New Yorker,* August 2020.

Q: Are GNSS vulnerabilities being exploited in the wild, or are they only laboratory phenomena?

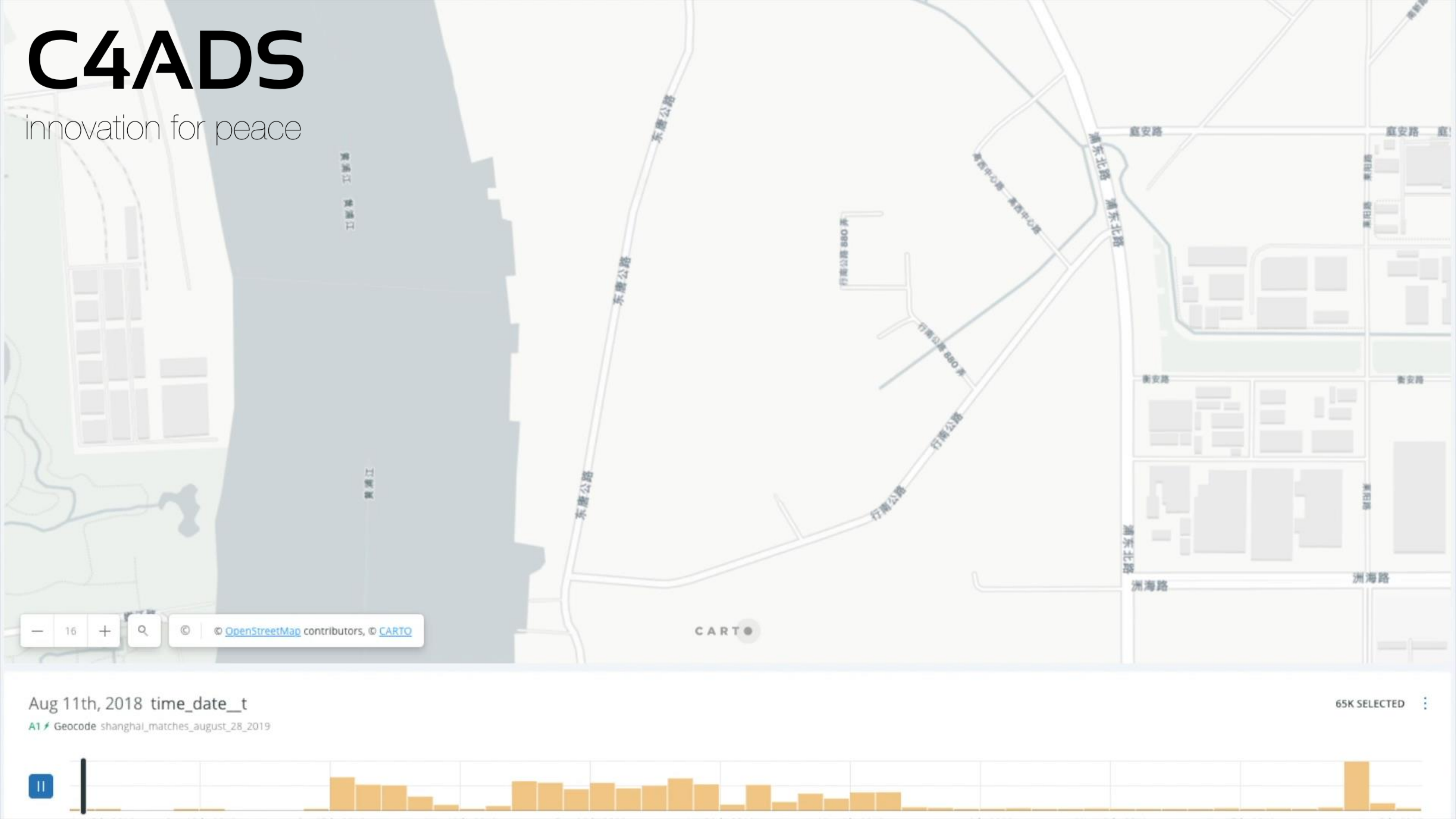
Black Sea Spoofing Activity

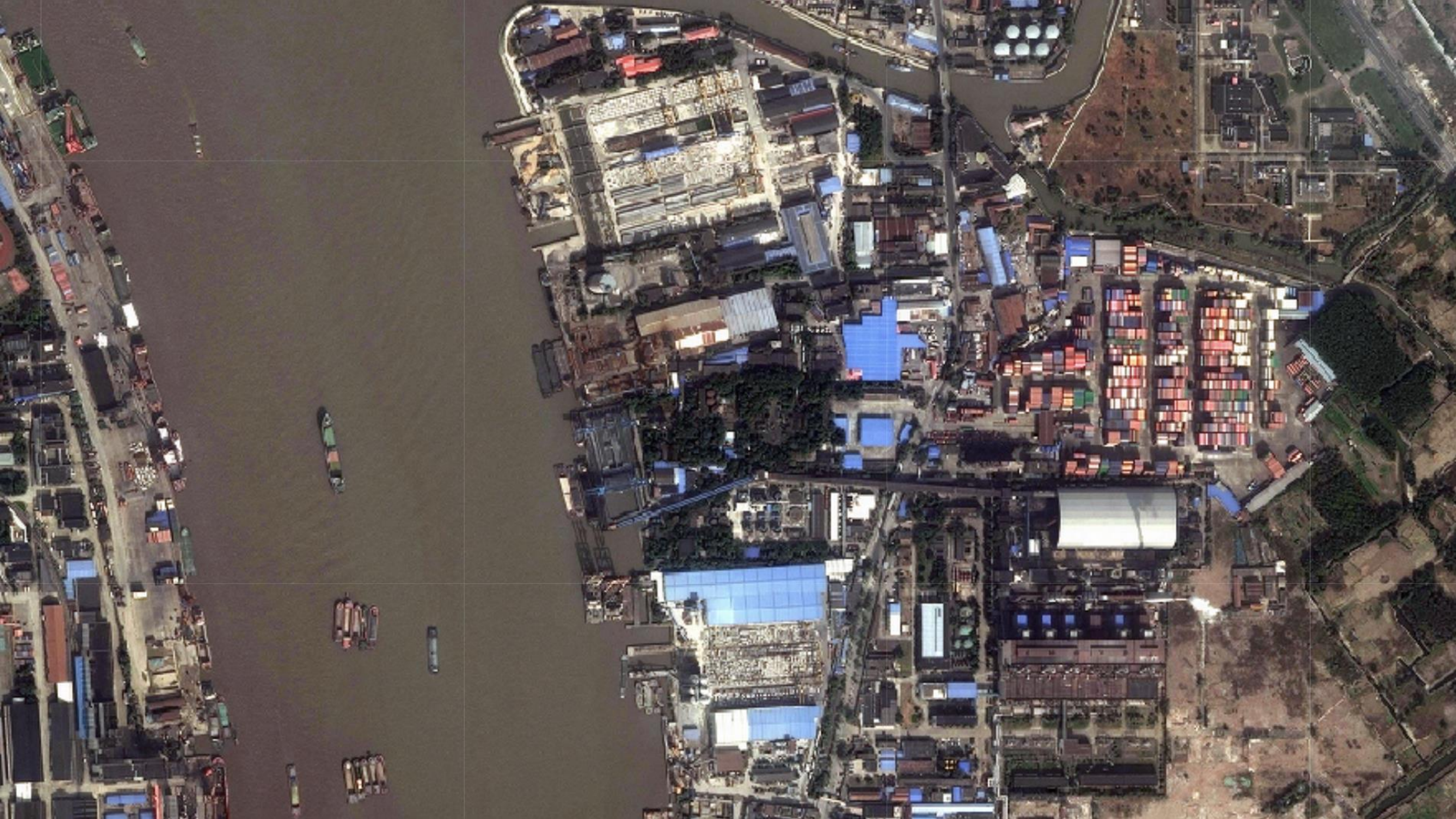
January 2016-November 2018

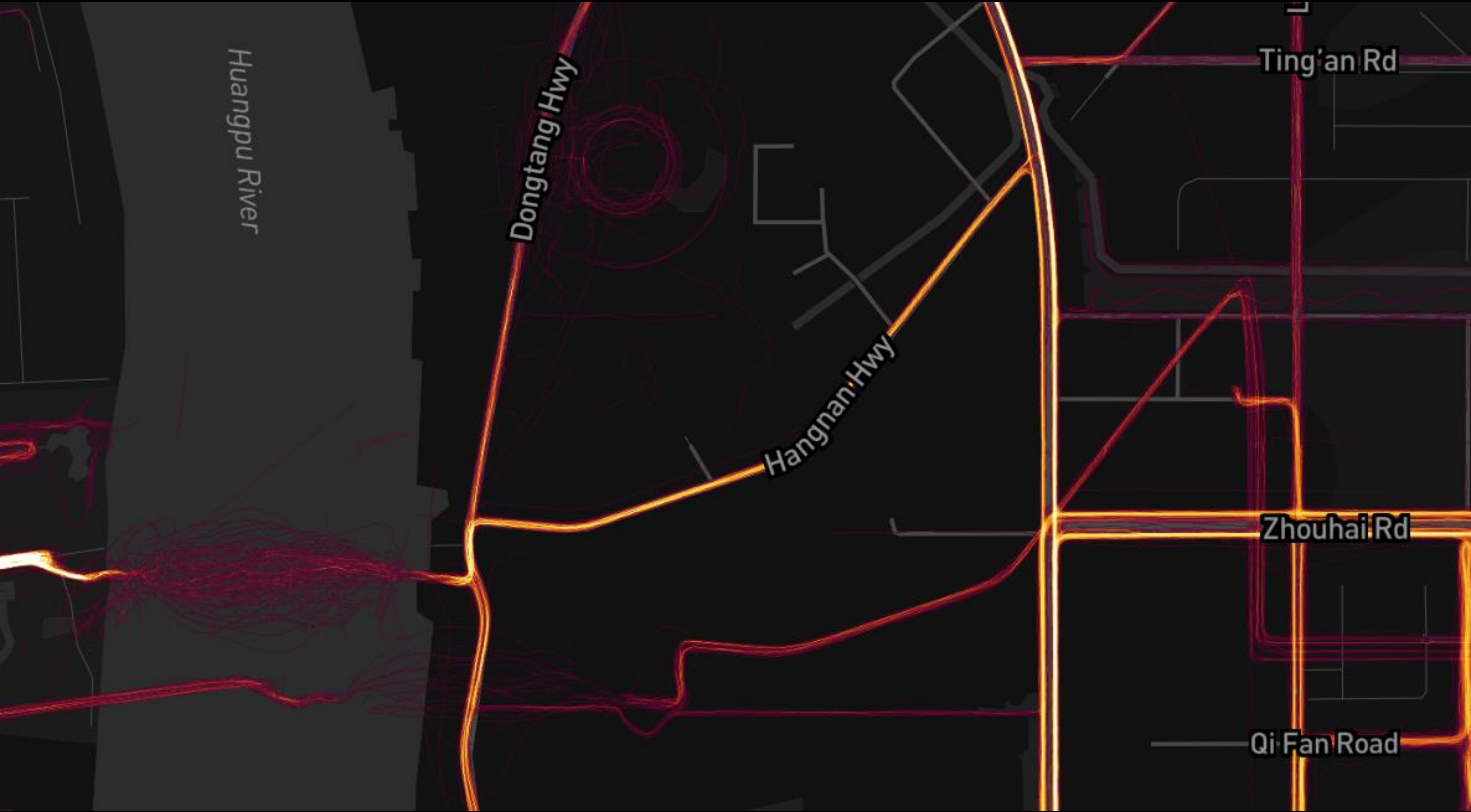
C4ADS "Above Us Only Stars: Exposing GPS Spoofing in Russia and Syria."

C4ADS innovation for peace

C4ADS
innovation for peace







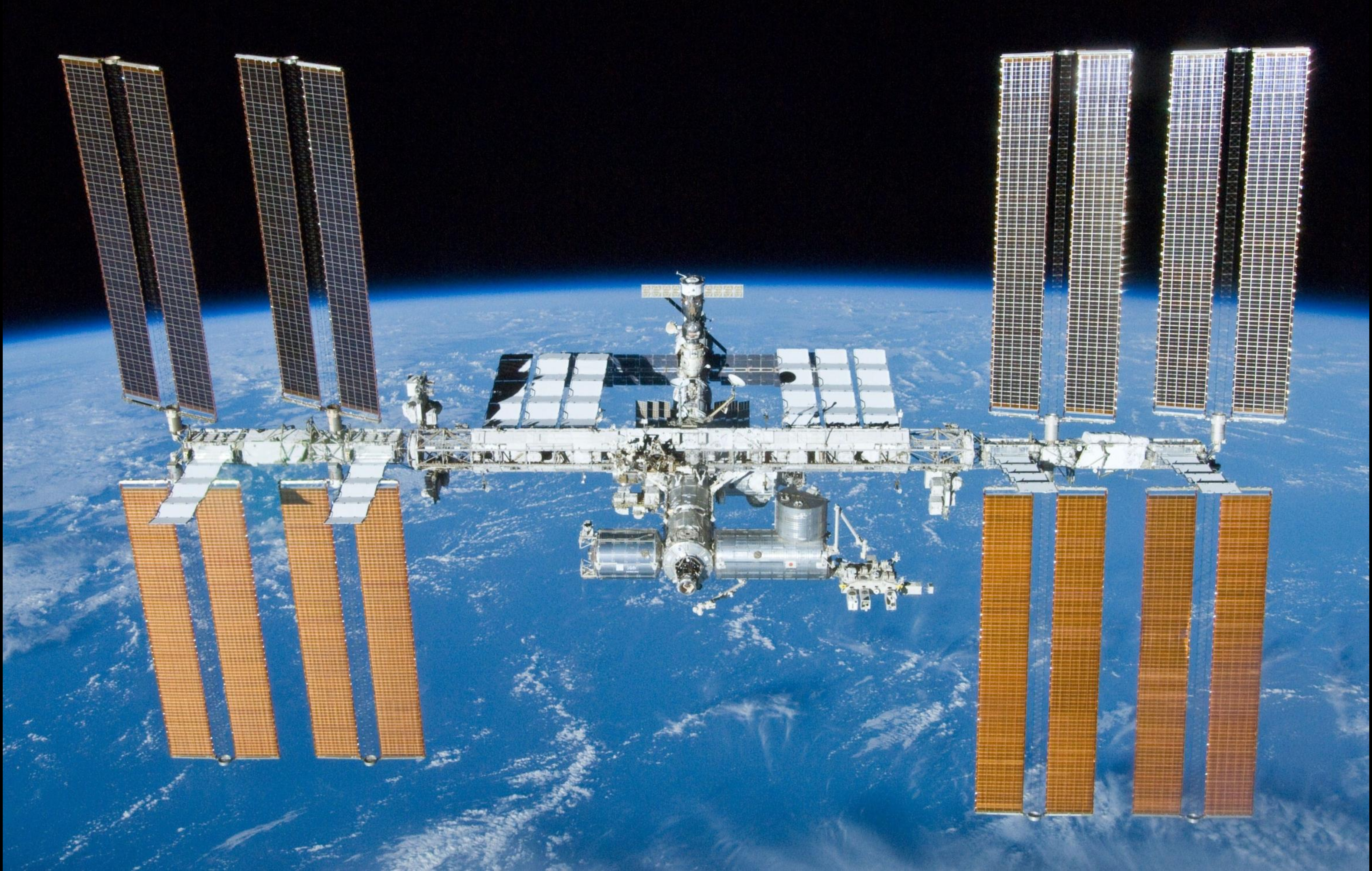
Huangpu River
Dongtang Hwy
Hangnan Hwy
Ting'an Rd
Zhouhai Rd
Qi Fan Road


Dongtang Hwy

Capable turnkey GNSS spoofer can now be purchased for less than $300

Q: Can LEO SVs be used for global GNSS interference monitoring?

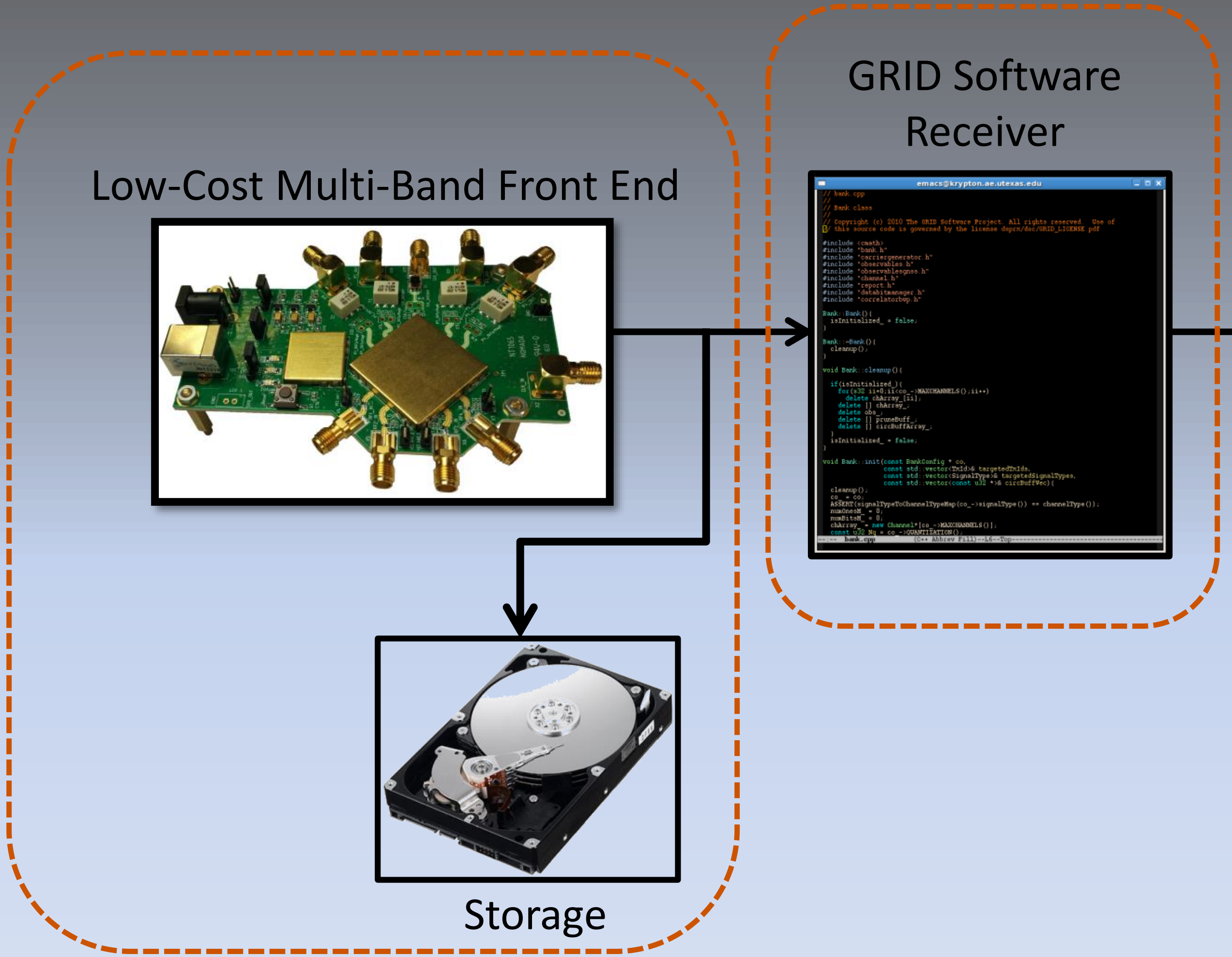
A flexible, science-grade GNSS receiver in low-earth orbit (LEO) would enable continuous global monitoring and characterization of GNSS interference

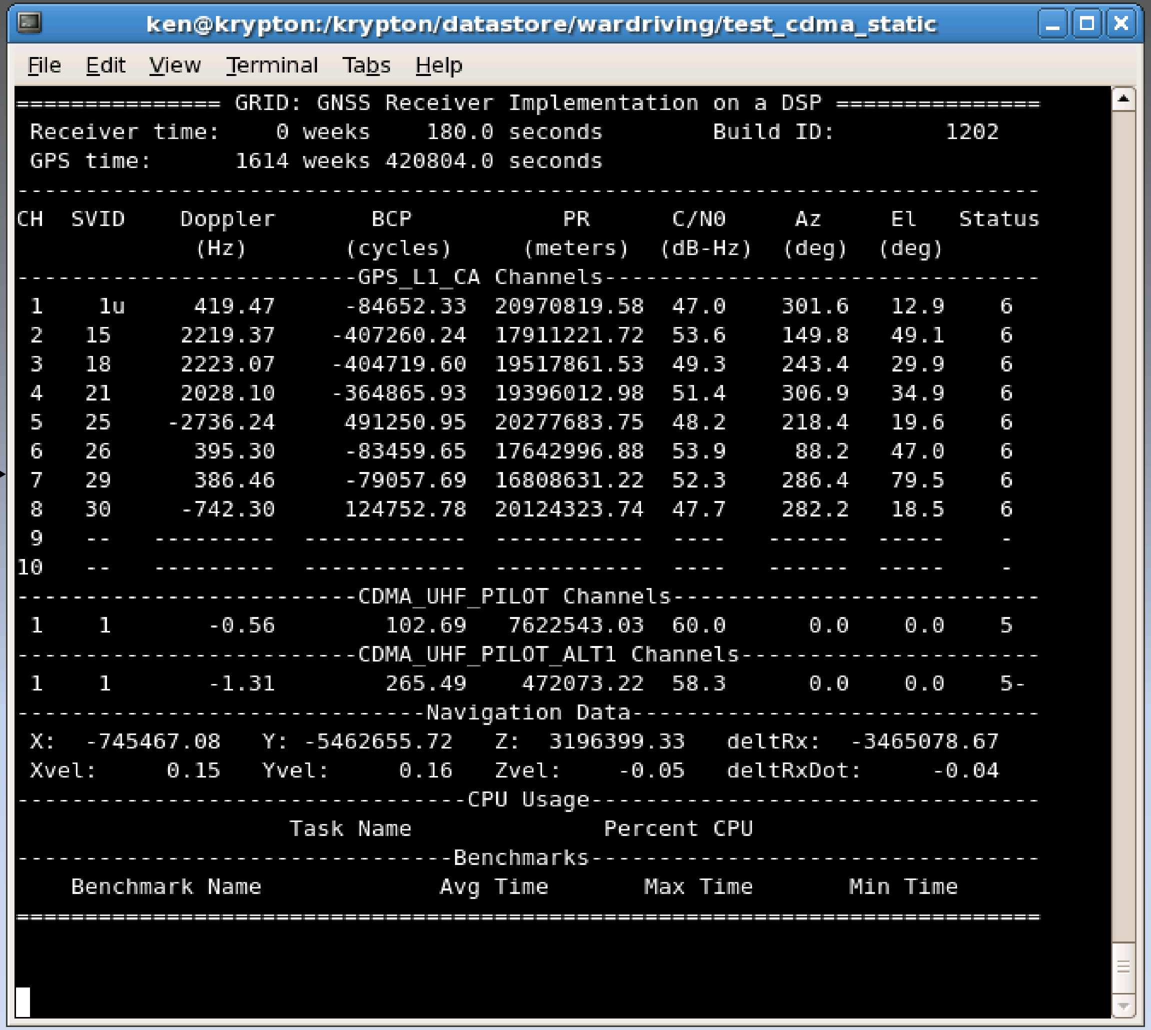


February 2017: FOTON SDR installed on International Space Station

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

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





```
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 14 years of development.

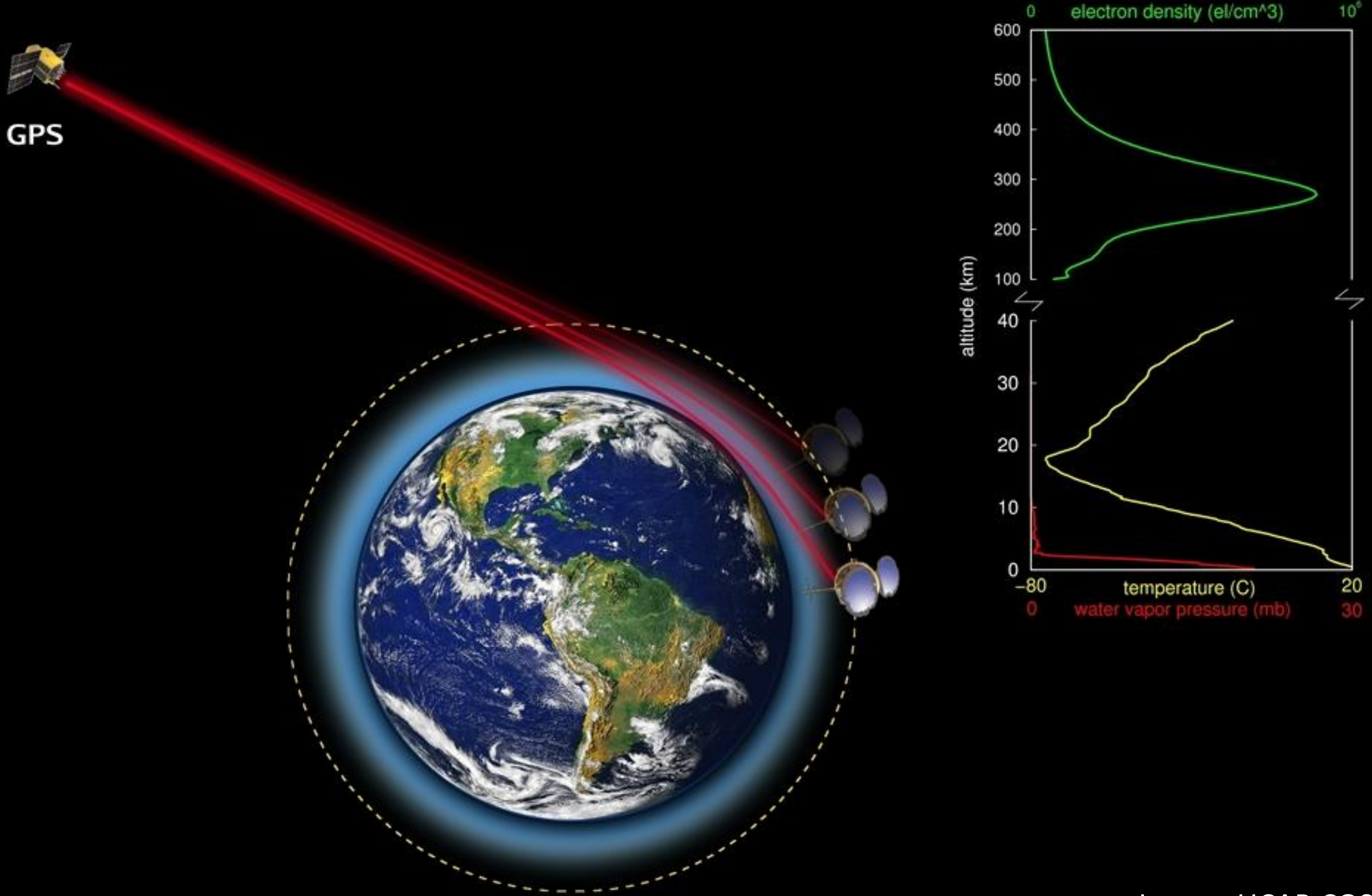
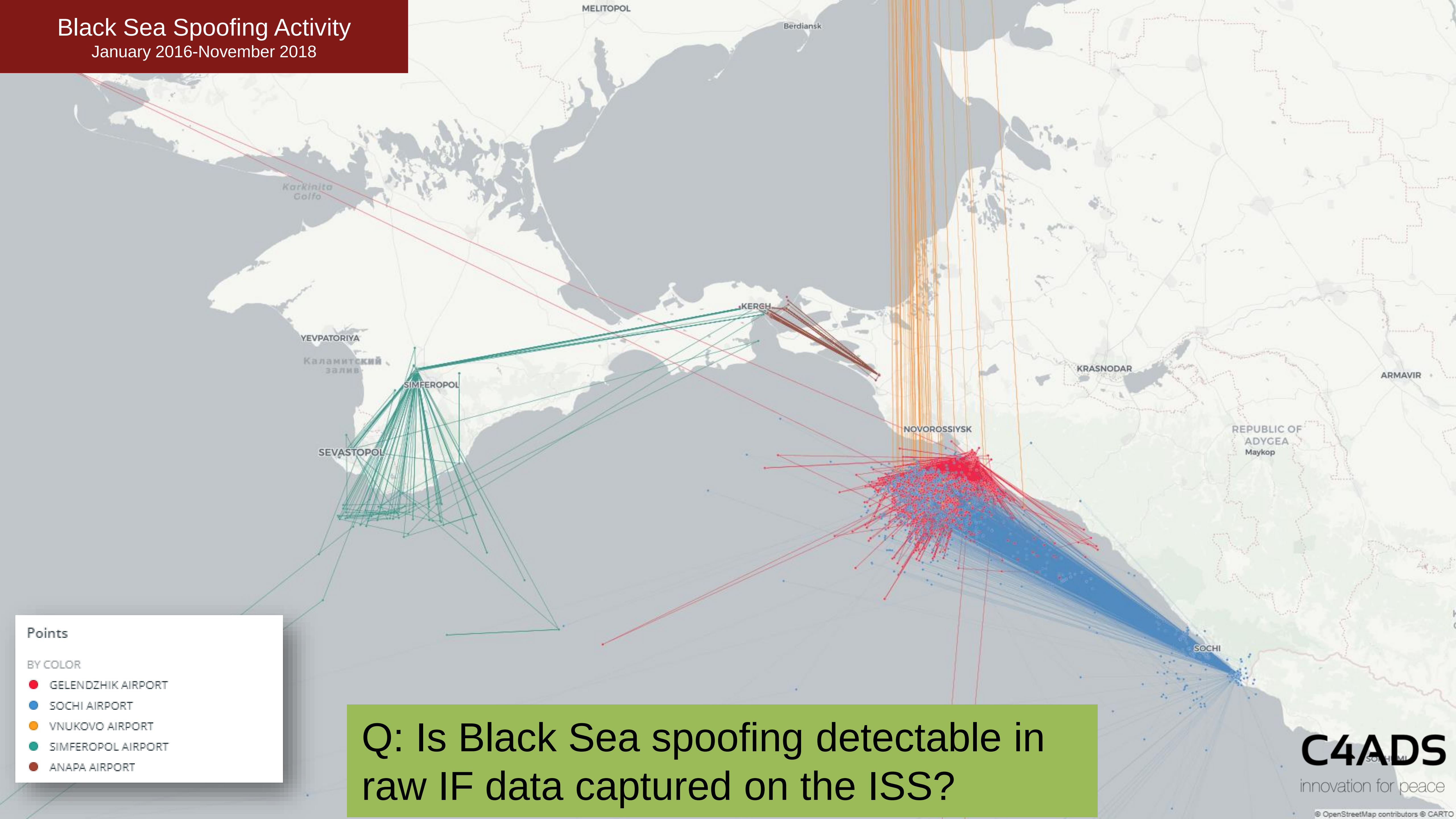


Image: UCAR COSMIC Program

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

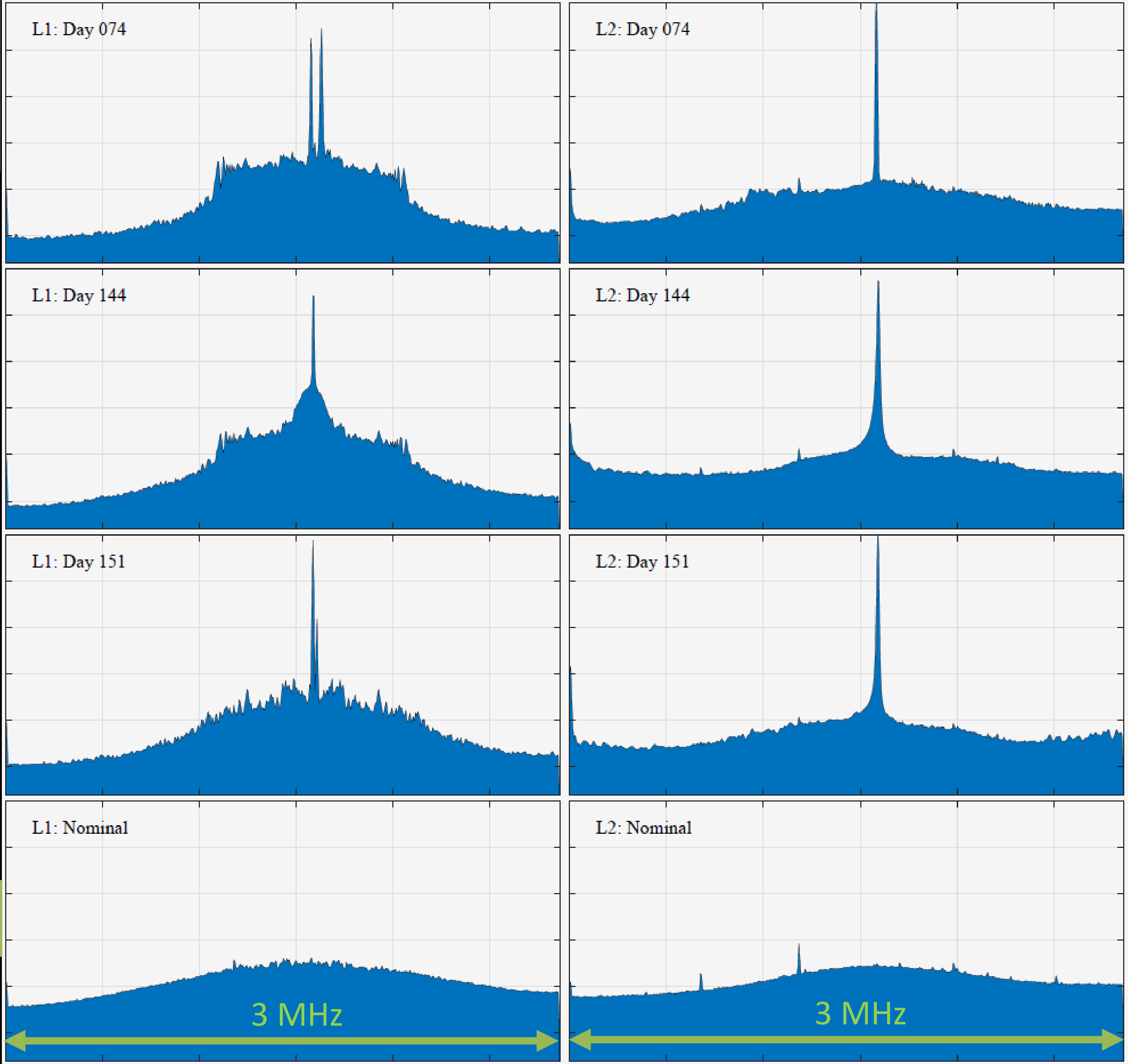
March-May 2018: Raw IF samples captured near Black Sea on 3 separate days

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

Power Spectra

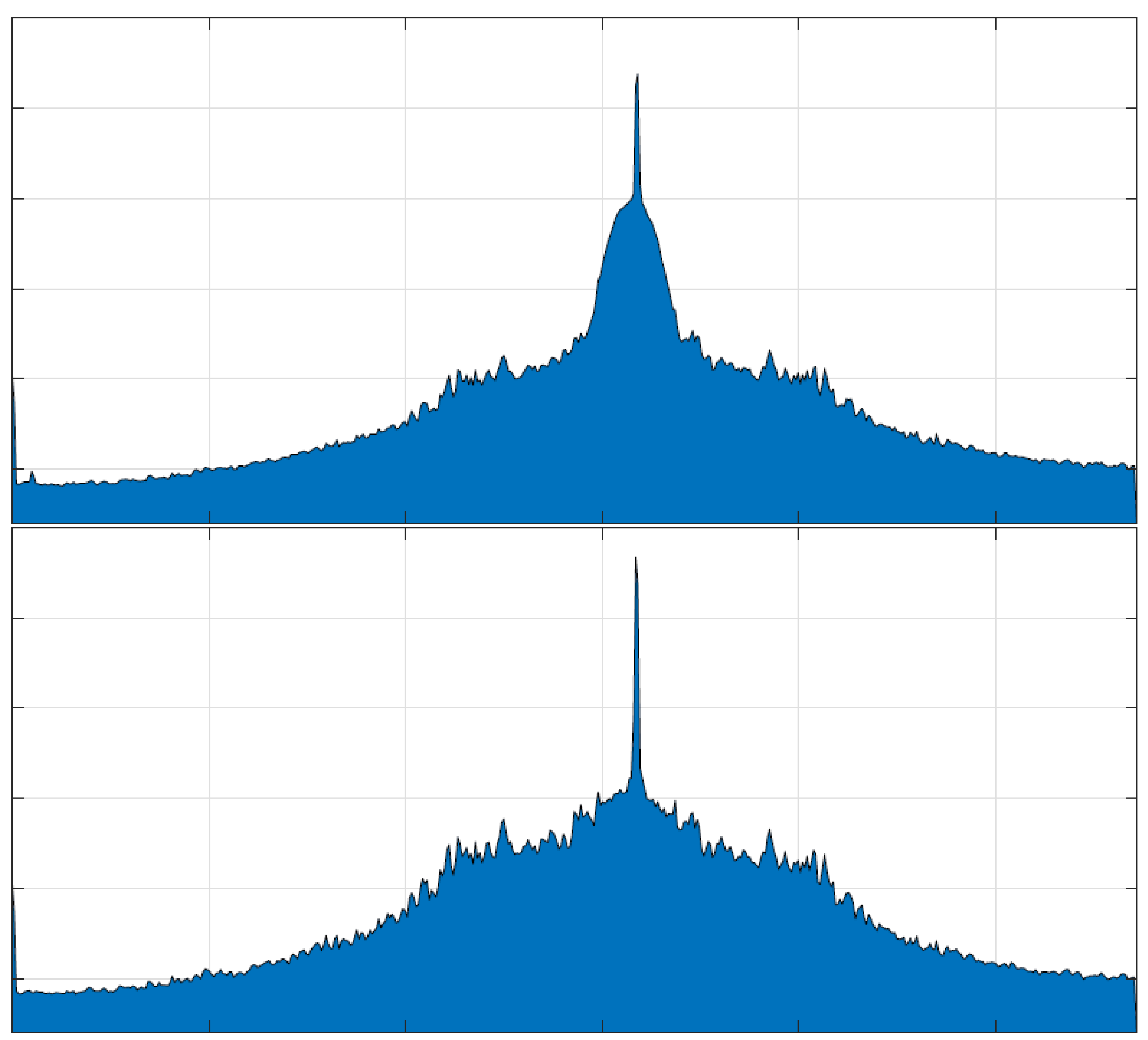
L1: 1575.42 MHz

L2: 1227.6 MHz



Maximum

Minimum



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

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	[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

“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).

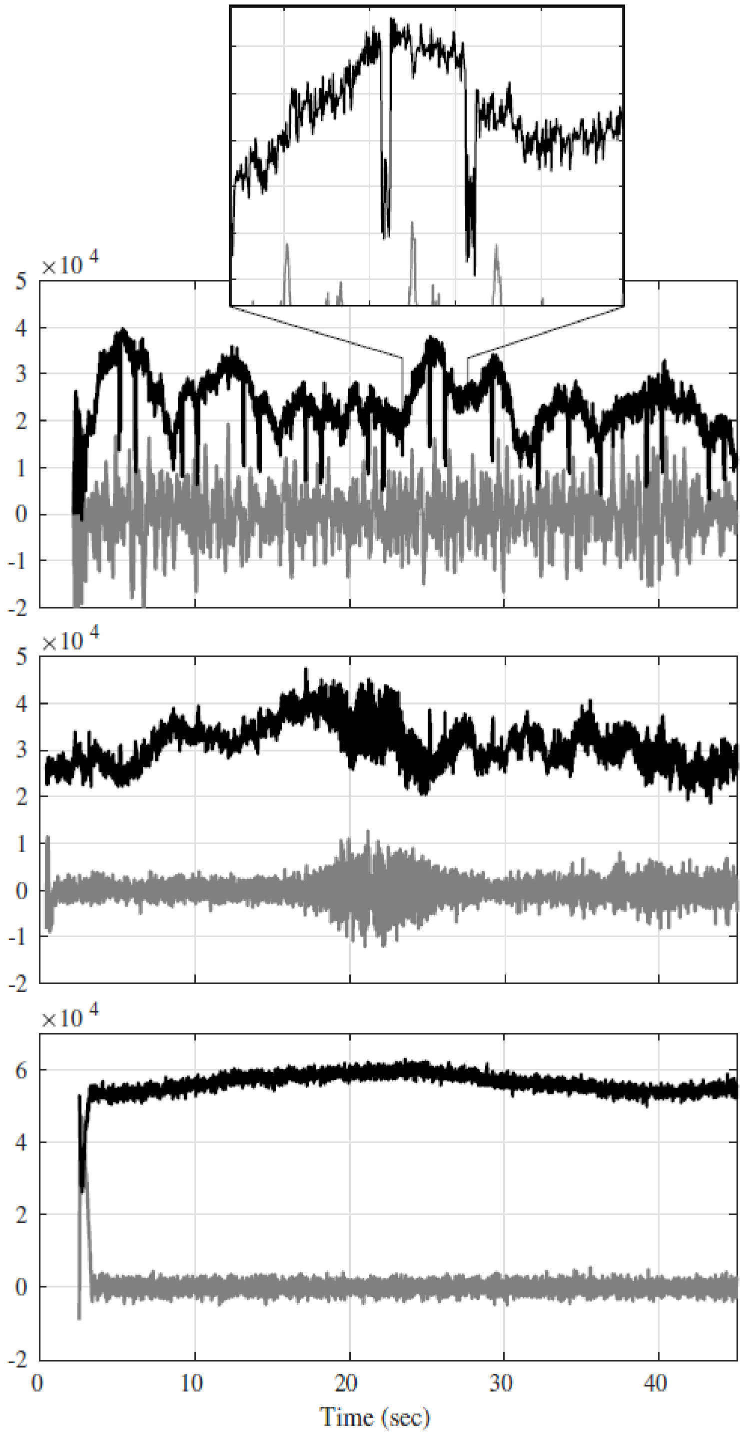
Data-Wiped 100-Hz IQ accumulations

Unexplained fading

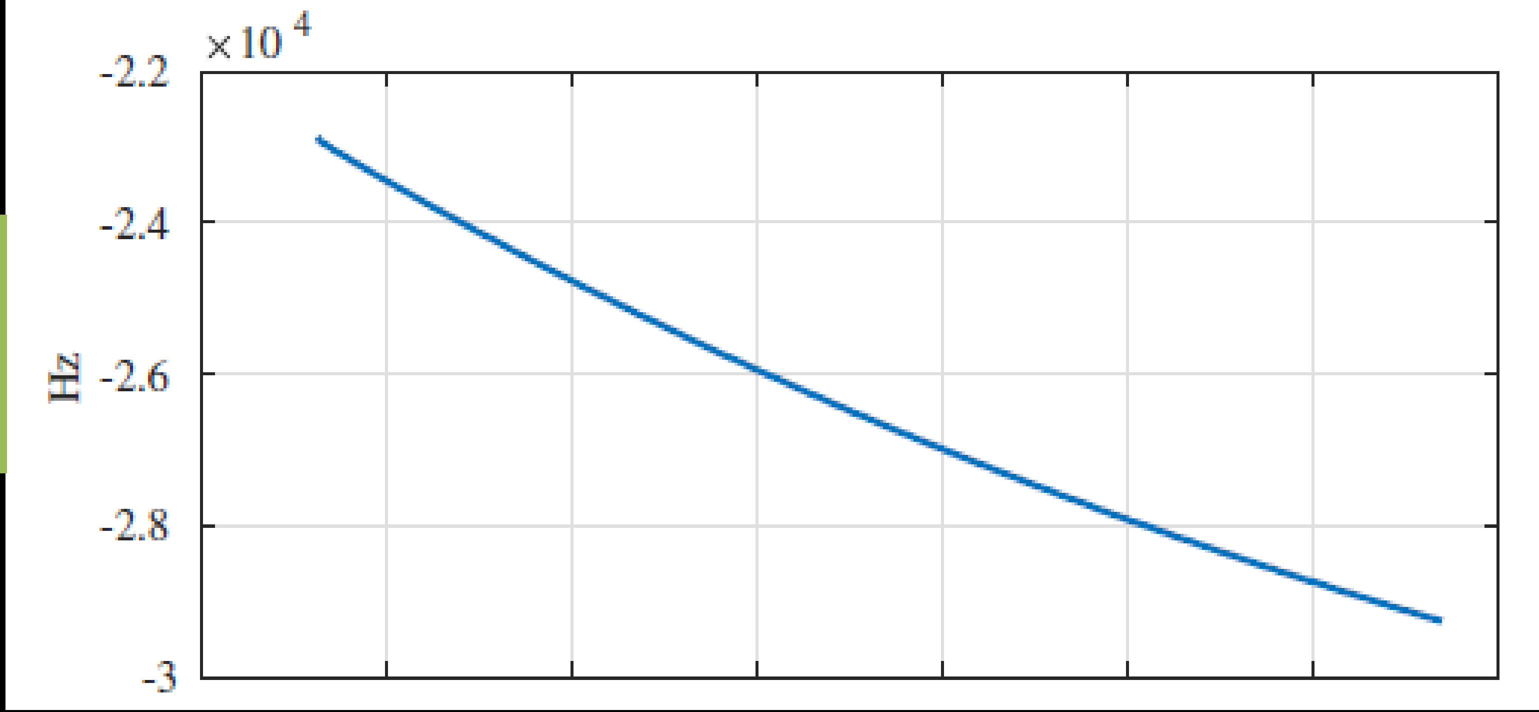
False signal

Authentic signal in interference

Authentic signal under clean conditions



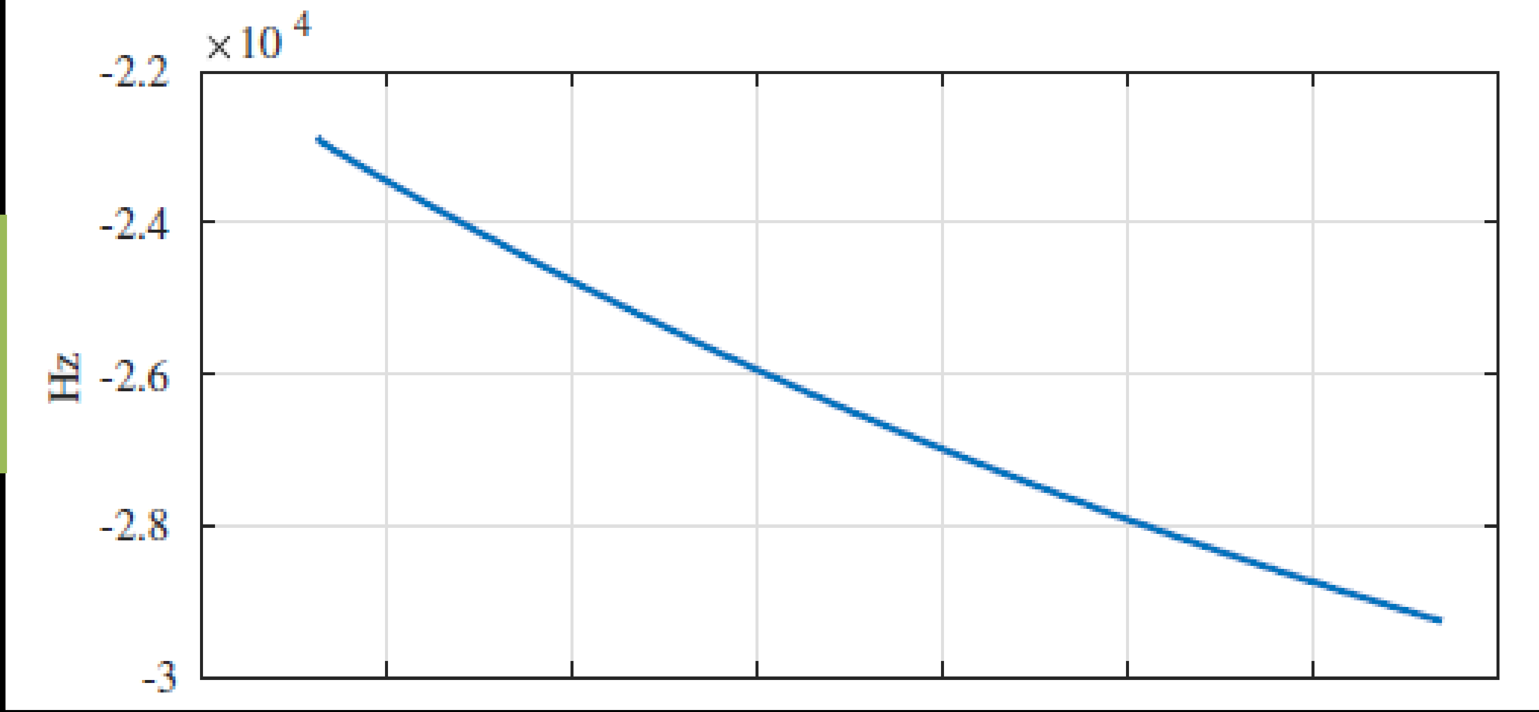
Doppler time history for false PRN 10 signal from day 144 capture



Doppler model nonlinearly related to transmitter position, but also strongly affected by transmitter clock error rate.

$$f_{\mathrm{D}} = -\hat{\boldsymbol{r}}^{T} \boldsymbol{v}_{\mathrm{R}} / \lambda - c \left[\delta \dot{t}_{\mathrm{R}} - \delta \dot{t}_{\mathrm{T}} \left(1 - \delta \dot{t}_{\mathrm{R}} \right) \right] / \lambda + w$$

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

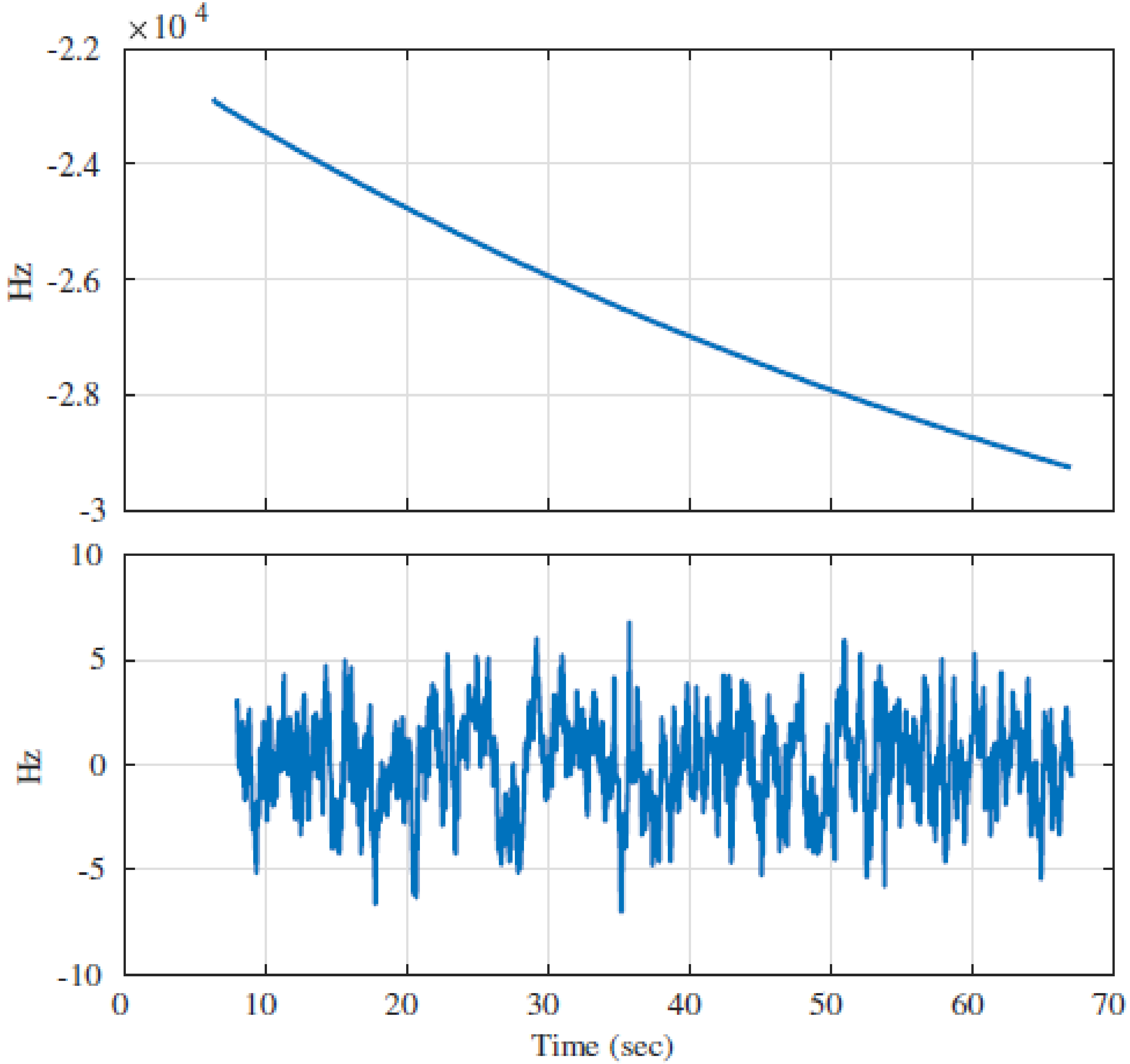


Marginal contribution of TX frequency instability to a single-pass geolocation error ellipse semi major (a) and semi minor (b) axes

Clock Quality	h_{-2}	a (m)	b (m)
TCXO	3×10^{-21}	6900	690
Low-quality OCXO	3×10^{-23}	720	72
OCXO	3×10^{-25}	67	7.4

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

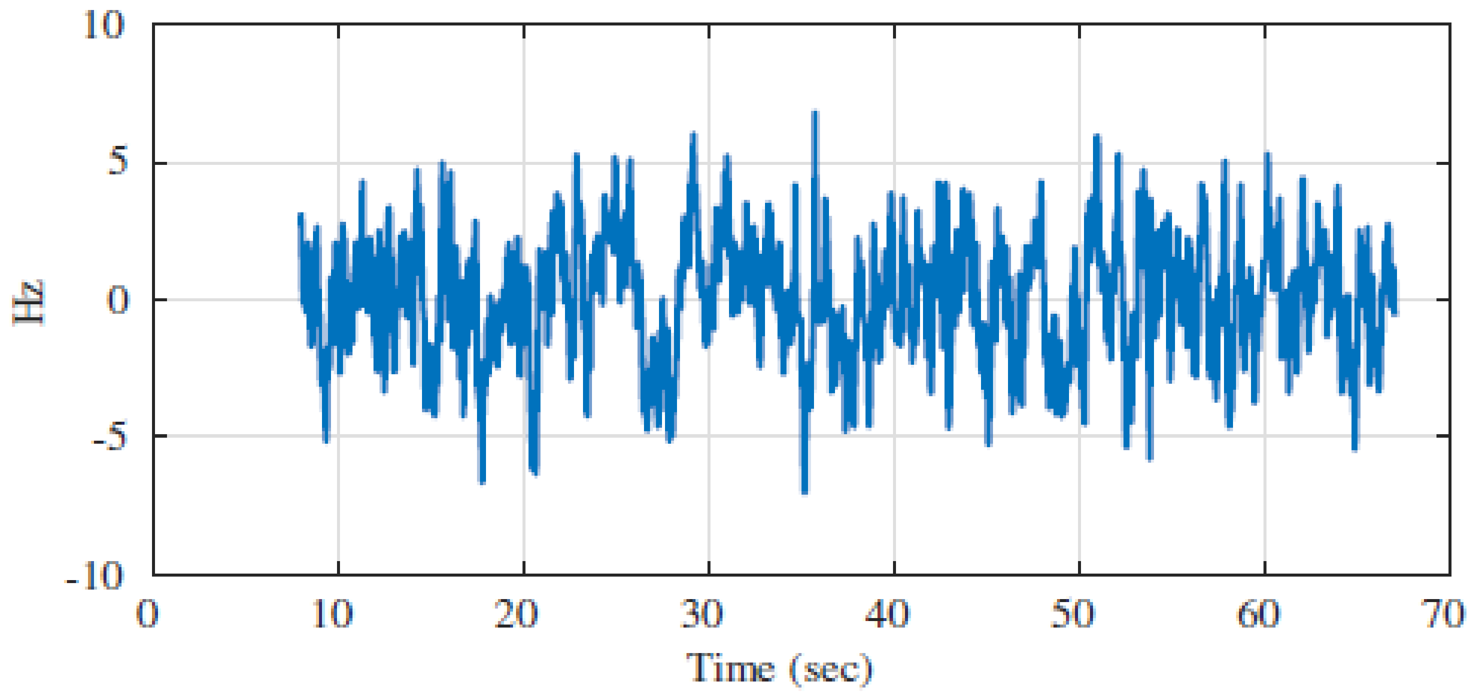
Post-fit residuals of Doppler time history assuming estimated transmitter location and clock rate offset

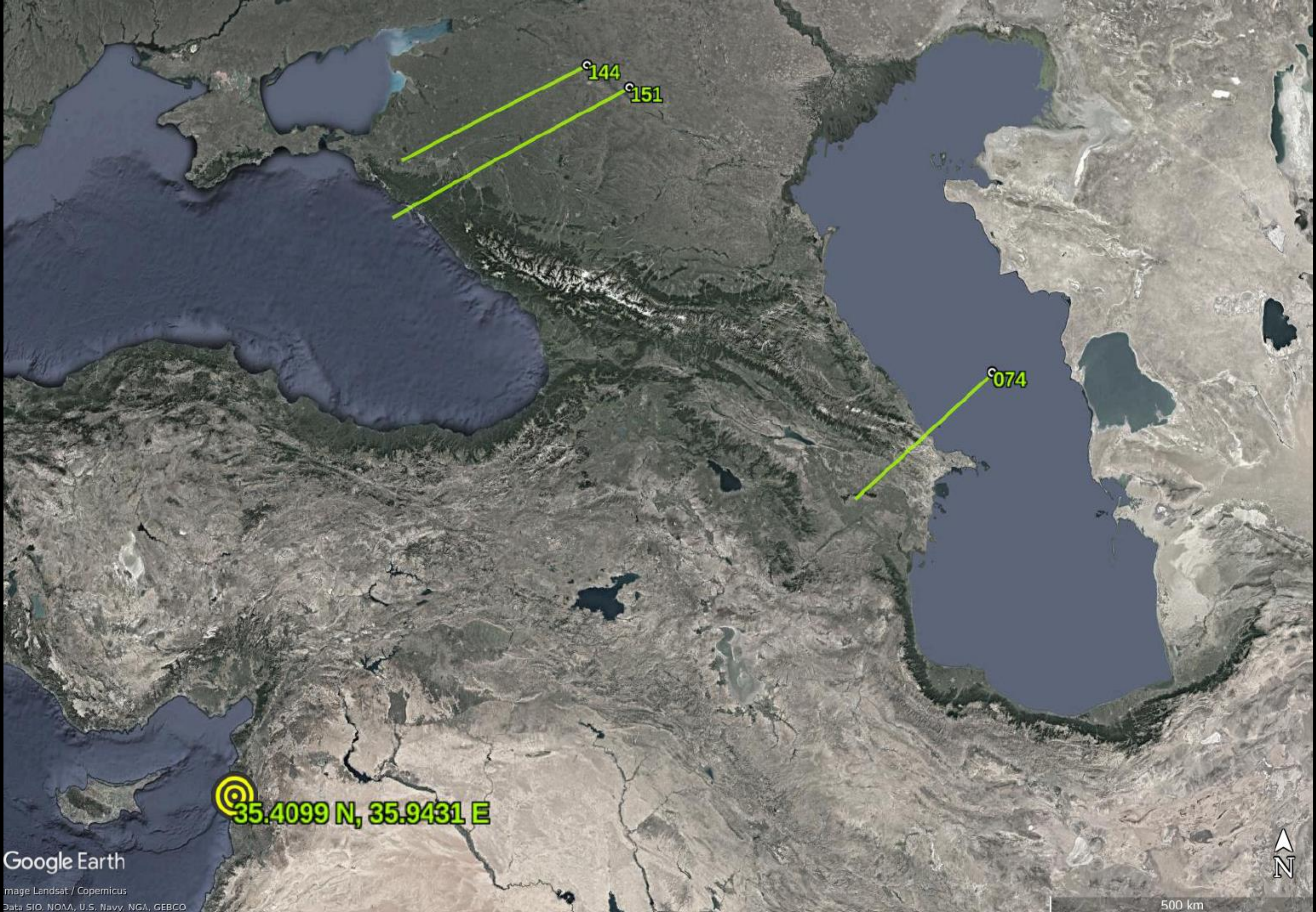


Analysis of the estimated clock frequency rate for days 74 and 144 revealed an Allan deviation consistent with an OCXO

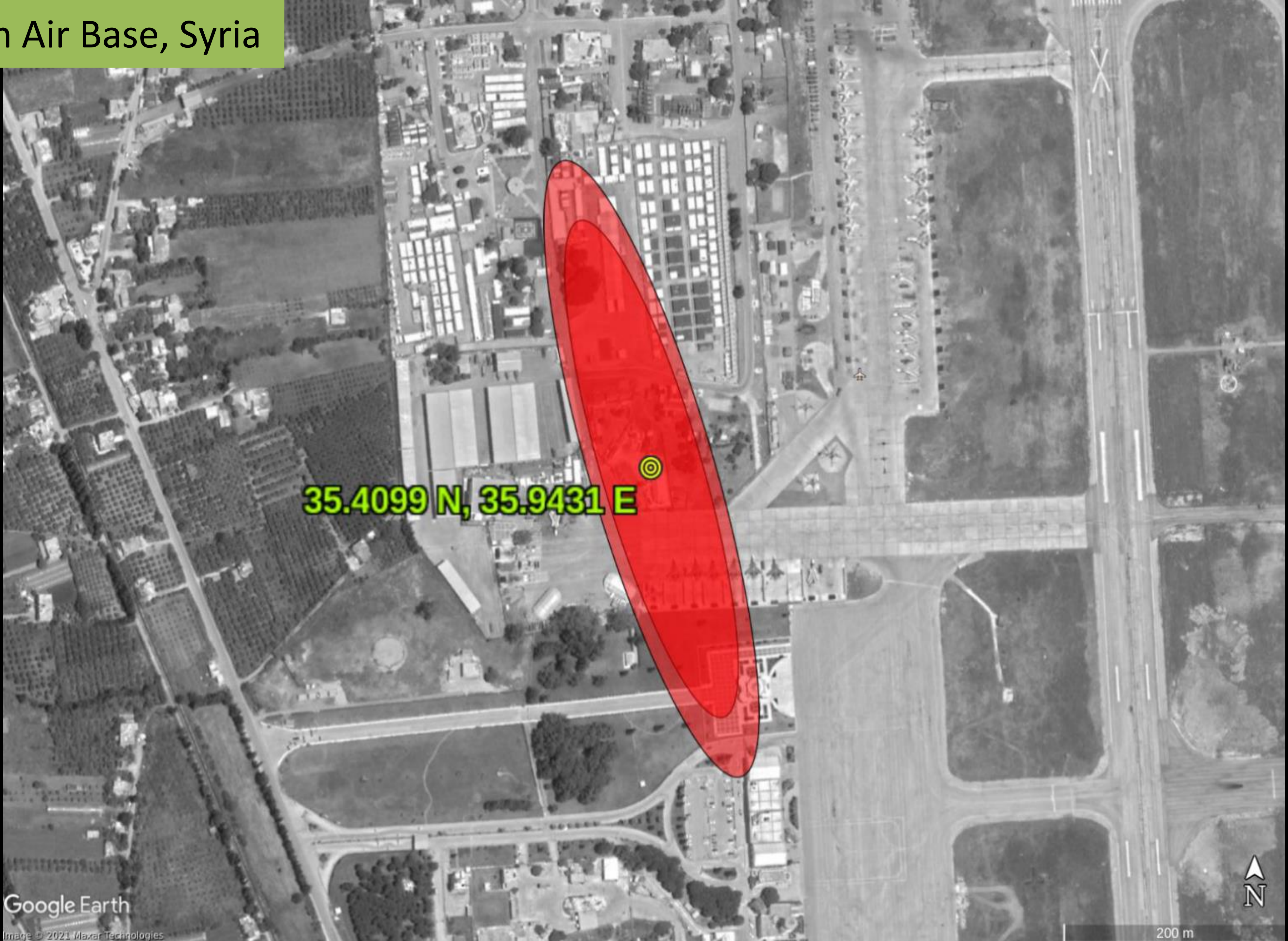
$$\sigma_y(2, \tau, \tau) = 1.6 \times 10^{-11}$$

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

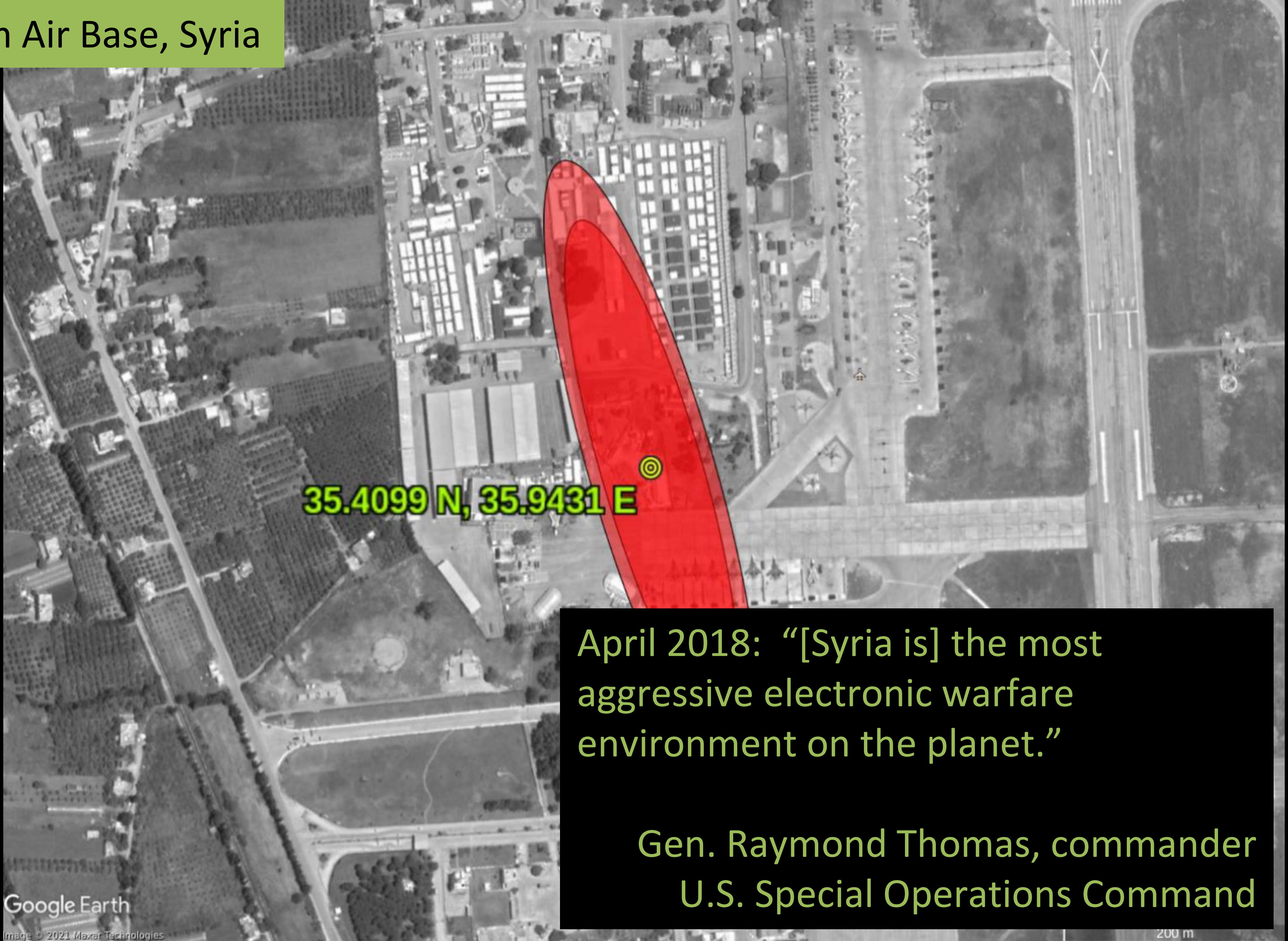



144
151
074
35.4099 N, 35.9431 E
Google Earth
Image Landsat / Copernicus
Data SIO, NOAA, U.S. Navy, NGA, GEBCO
500 km
N

Khmeimim Air Base, Syria

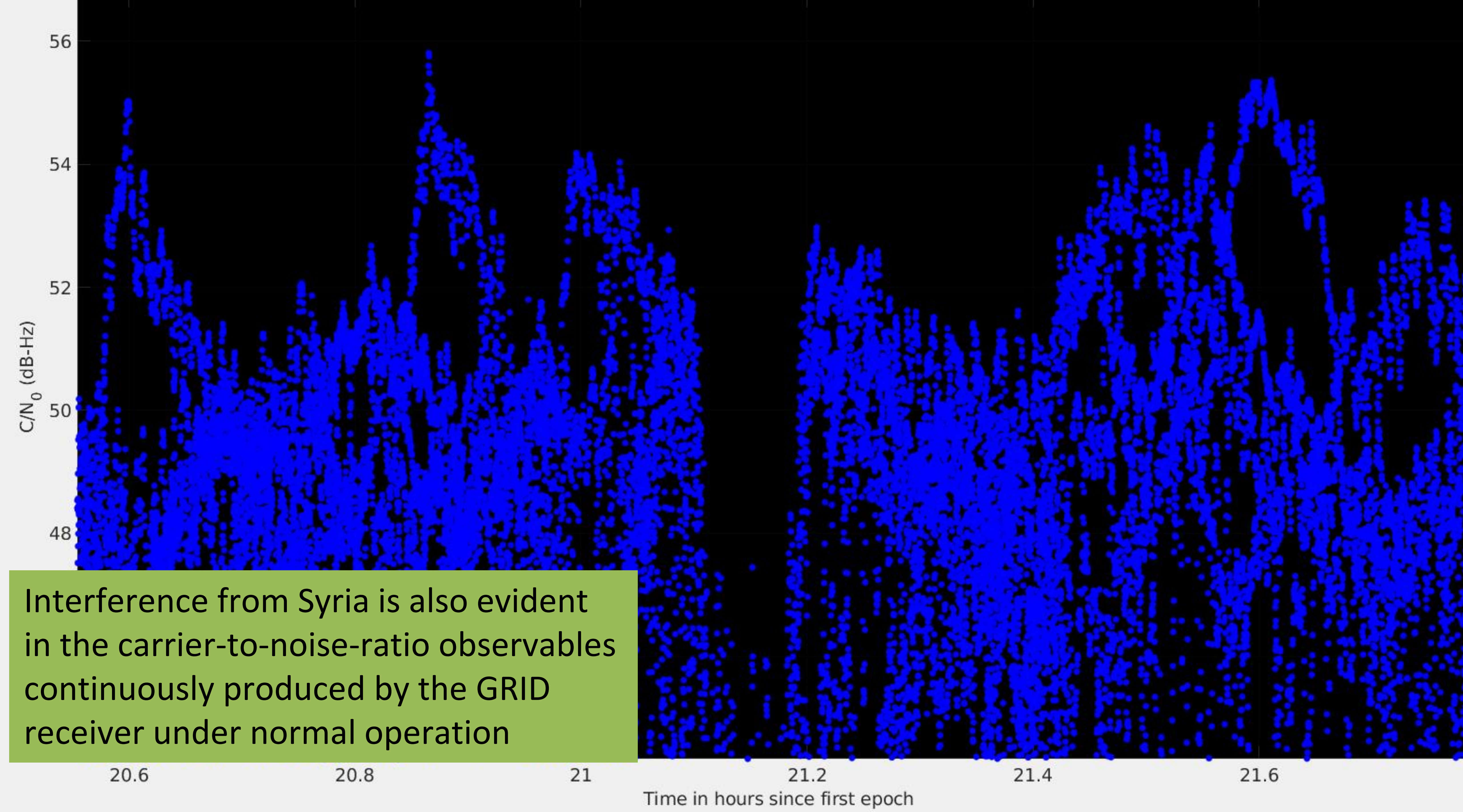


Khmeimim Air Base, Syria



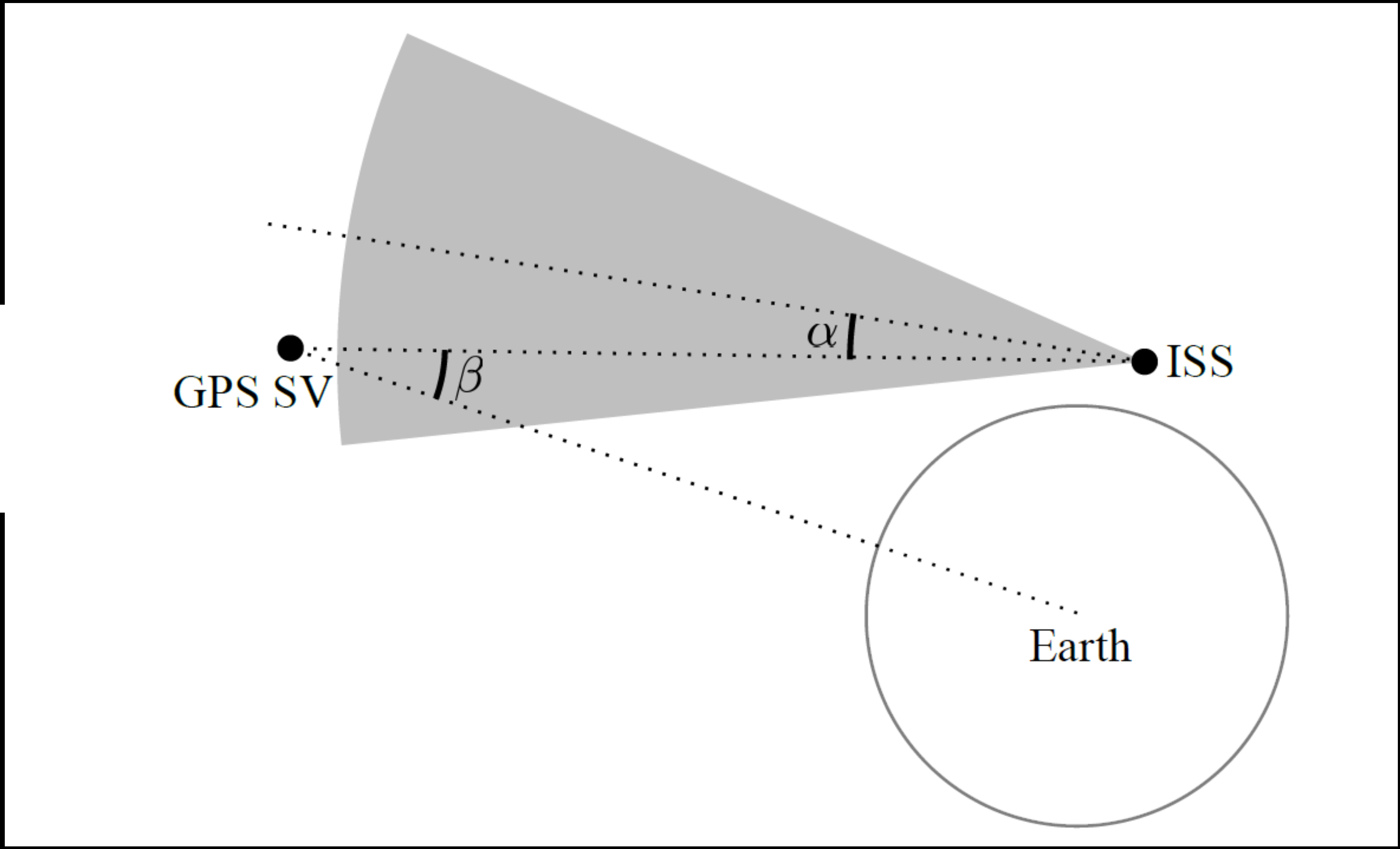
April 2018: "[Syria is] the most aggressive electronic warfare environment on the planet."

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

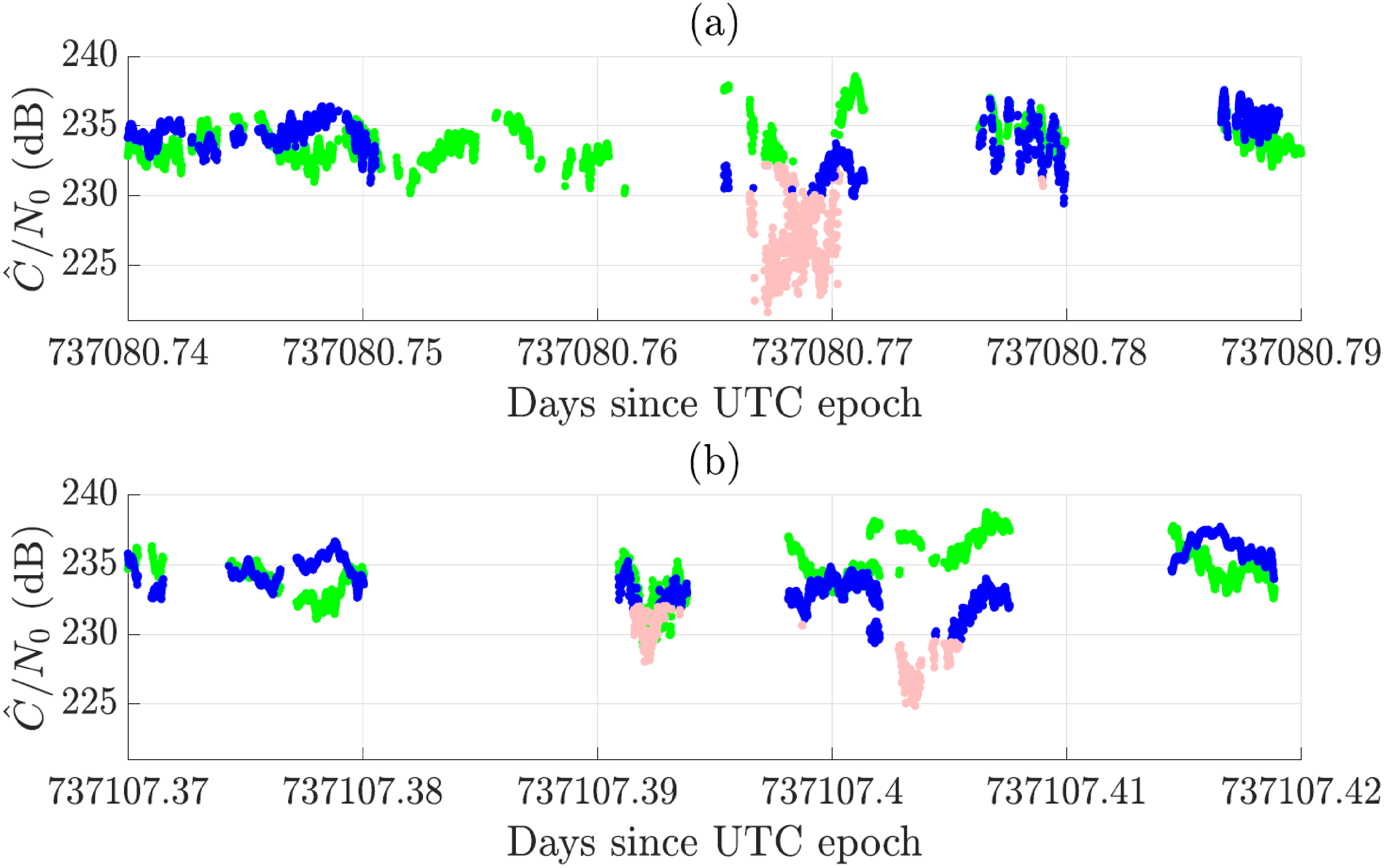


Interference from Syria is also evident in the carrier-to-noise-ratio observables continuously produced by the GRID receiver under normal operation

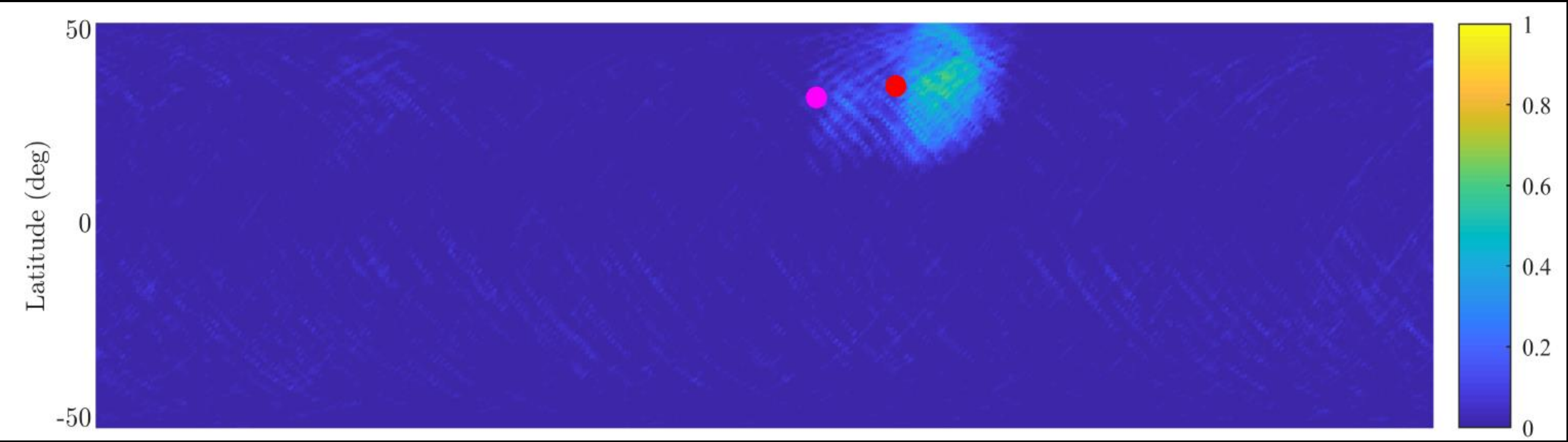
$$C(j, f, r_{sr}, z_s, z_r)$$



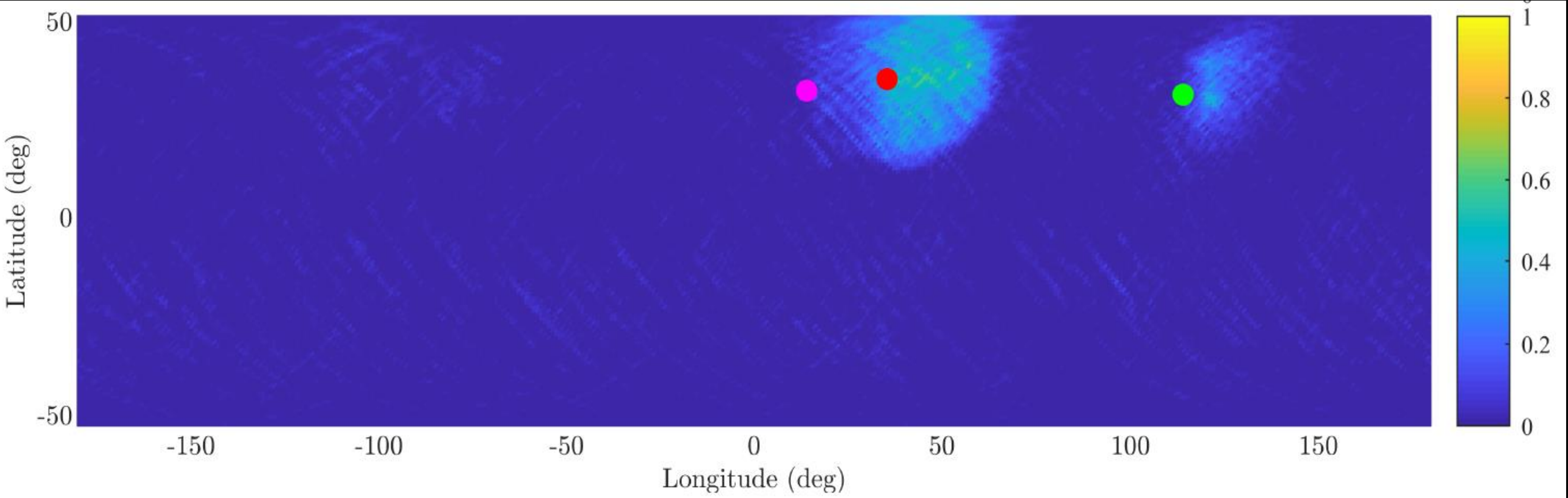
To maximize detectability, CINR observations must be pre-processed to compensate for predictable variations due to PRN (j), frequency (f), range (r_{sr}), satellite off-boresight angle (z_s), and receiver off-boresight angle (z_r).



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 March 2017 to June 2020. The interference source in Syria is clearly evident, with a pattern asymmetry due to the receiver's antenna pointing aft. A second source near Libya is also evident.



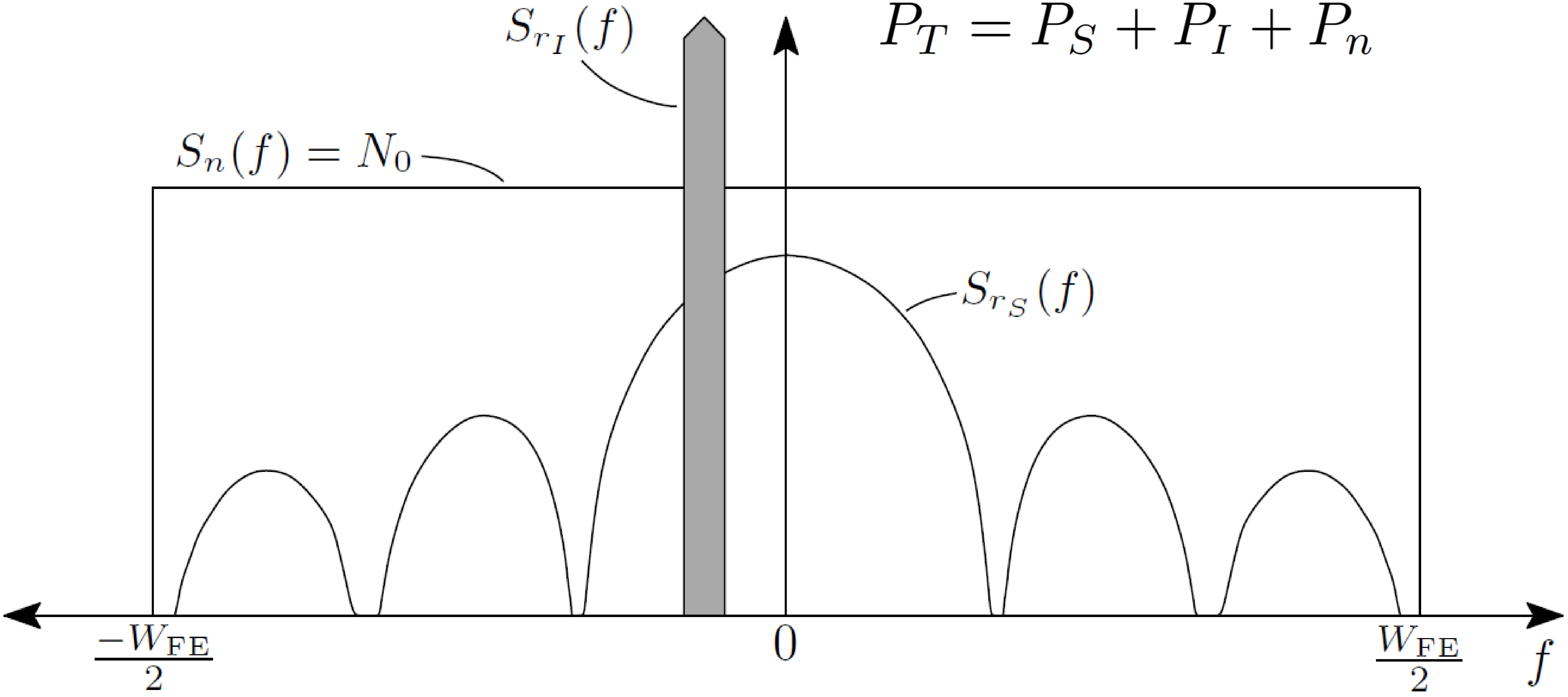
Heat map based on standard 1-Hz L2 C/N0 data from ISS GRID receiver from March 2017 to June 2020. Interference from Syria is evident, as is a persistent signature in mainland China at approximately 32 N, 114 E.

M. J. Murrian, L. Narula, P. A. Iannucci, S. Budzien, B. W. O'Hanlon, S. P. Powell, and T. E. Humphreys, "First results from three years of GNSS interference monitoring from low Earth orbit," Navigation, Journal of the Institute of Navigation, 2021. Submitted for review.

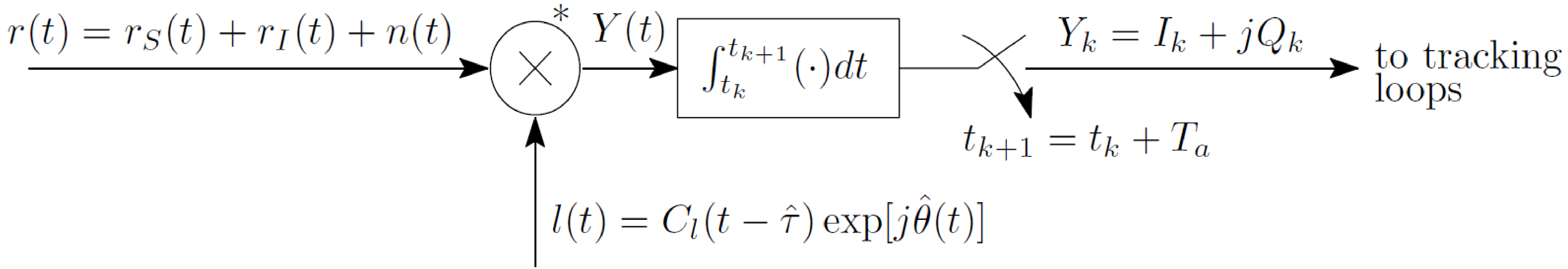
Q: How does one calculate the effect of a given interference waveform on an GNSS receiver?

$$r(t) = r_S(t) + r_I(t) + n(t)$$

$$P_T = P_S + P_I + P_n$$



Received signal is a mixture of signal, interference, and noise



$$I(t) = r_I^*(t) C_l(t - \hat{\tau}) \exp[j\hat{\theta}(t)]$$

$$S_I(f) = S_{C_l}(f) \star S_{r_I}(f) \star \delta(f + \hat{f}_D)$$

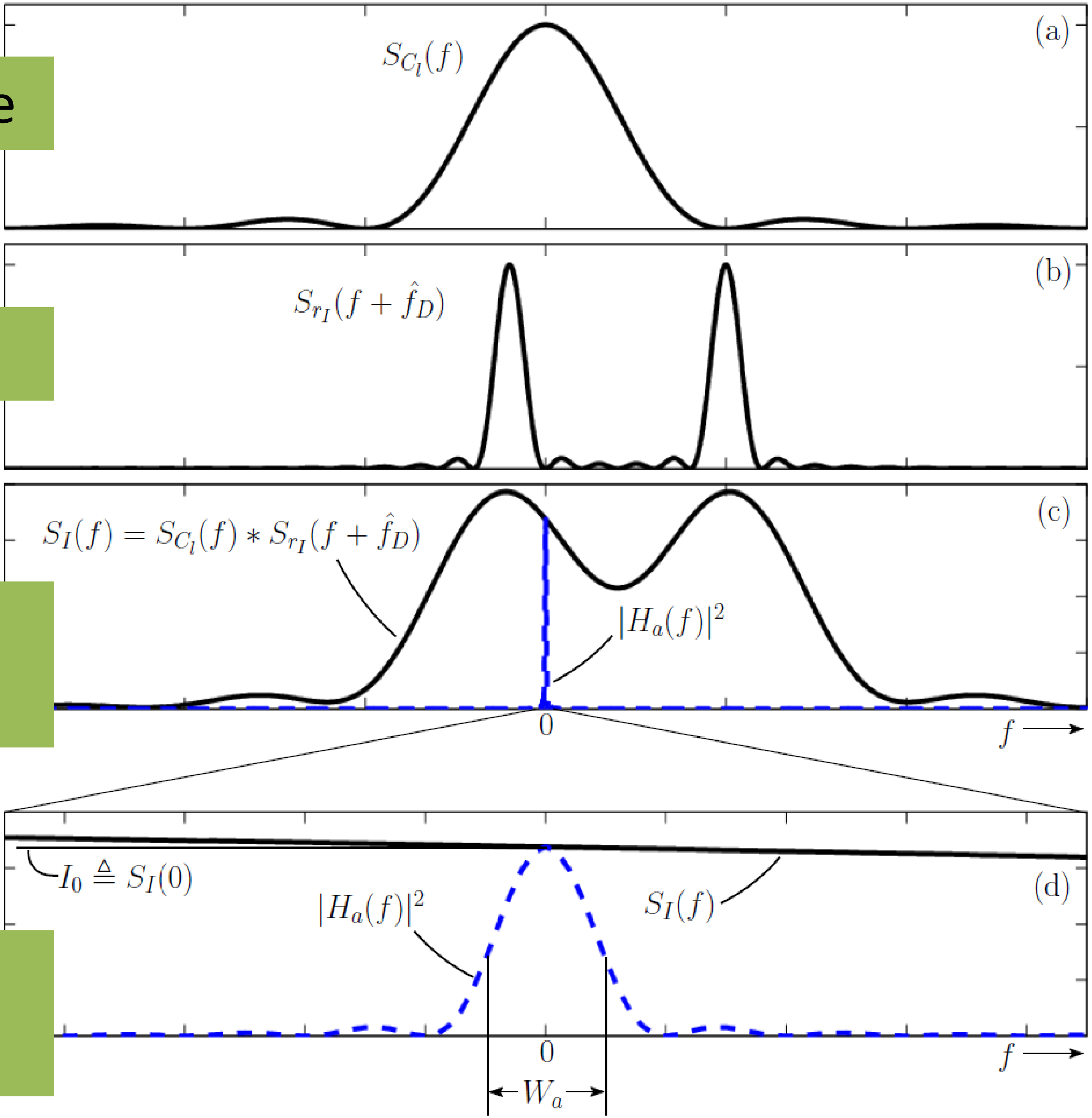
Received signal is multiplied by a local replica and accumulated. In the frequency domain, the interference component of Y(t) is a convolution of the psds of the desired code, the interference signal, and a delta fcn at the Doppler estimate.

psd of desired signal's spreading code

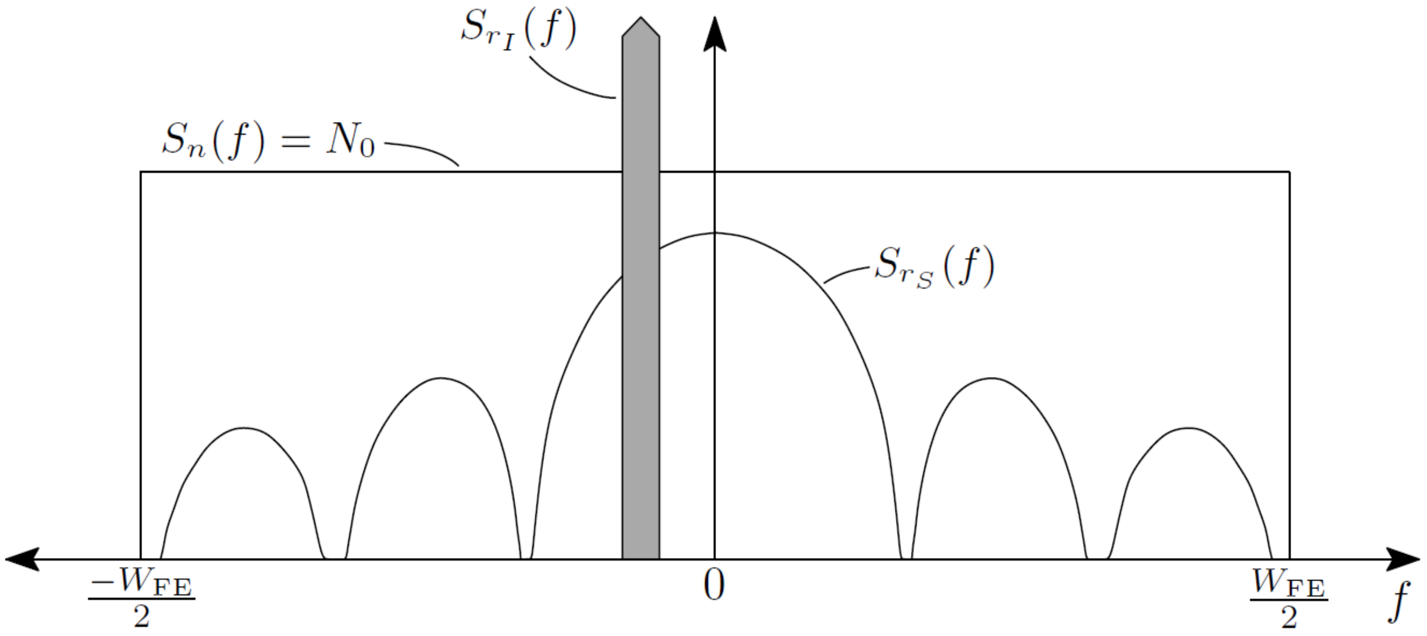
psd of interference signal

psd of $I(t)$, the interference component of $Y(t)$

I_0 is what makes it through into the receiver's tracking loops



$$\mathrm{CINR}_i = \frac{P_i}{N_0 + M_{0i} + I_0}$$



$$I_0 := \int_{-W_{\mathrm{FE}}/2}^{W_{\mathrm{FE}}/2} S_{r_I}(f) S_{C_l}(f)\ df$$

$$M_{0i} = \frac{2T_C}{3} \sum_{j \in \mathcal{I}(t) \setminus i} P_{\mathrm{A}j}$$

Q: What waveform is most potent for jamming? In other words, for a fixed interference power P_I what S_{r_I} maximizes I_0?

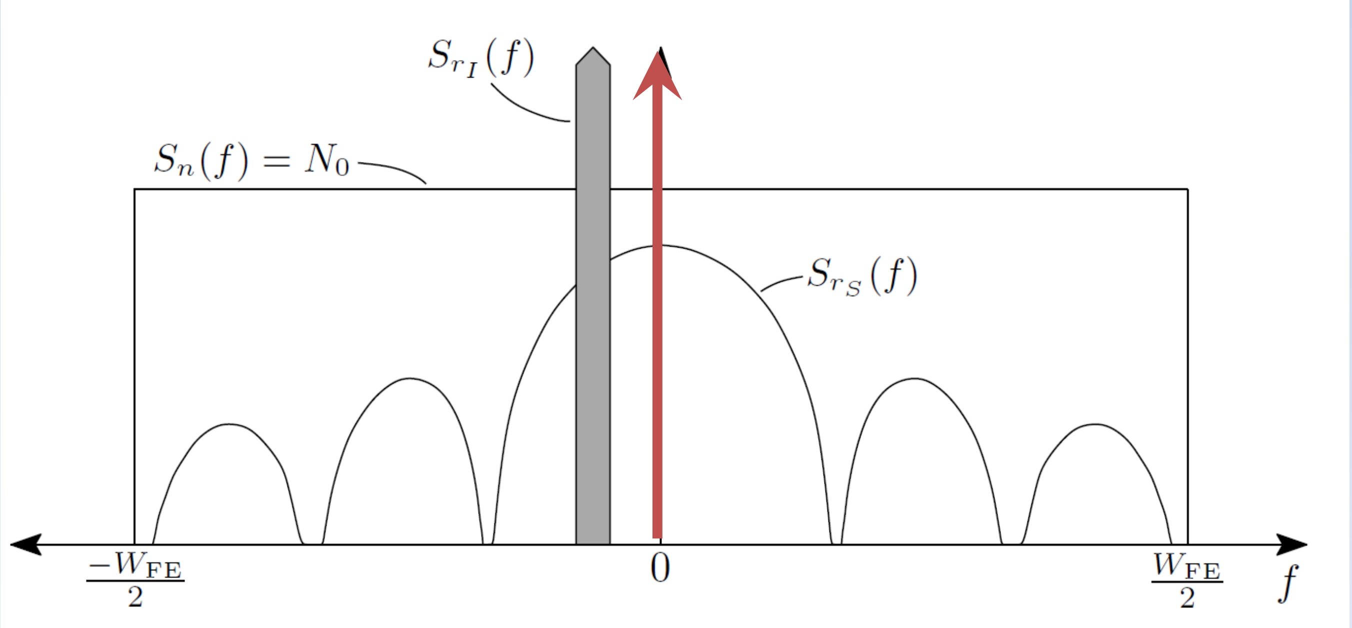
$$I_0 := \int_{-W_{\mathrm{FE}}/2}^{W_{\mathrm{FE}}/2} S_{r_I}(f) S_{C_l}(f) \; df$$

A: A pure tone jammer aligned with the highest point on the desired signal's psd:

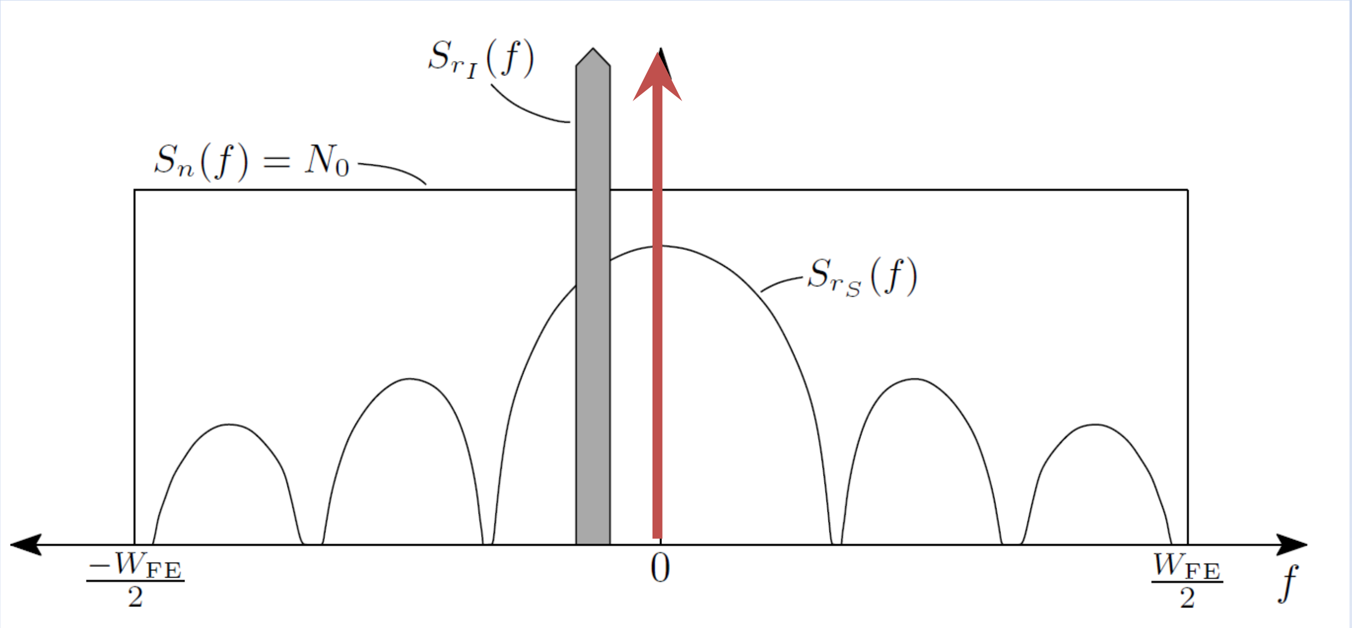
$$S_{r_I} = P_I \delta(\hat{f}_D)$$

$$I_0 := \int_{-W_{\mathrm{FE}}/2}^{W_{\mathrm{FE}}/2} S_{r_I}(f) S_{C_l}(f)\, df$$

$$\mathrm{CINR}_i = \frac{P_i}{N_0 + M_{0i} + I_0}$$

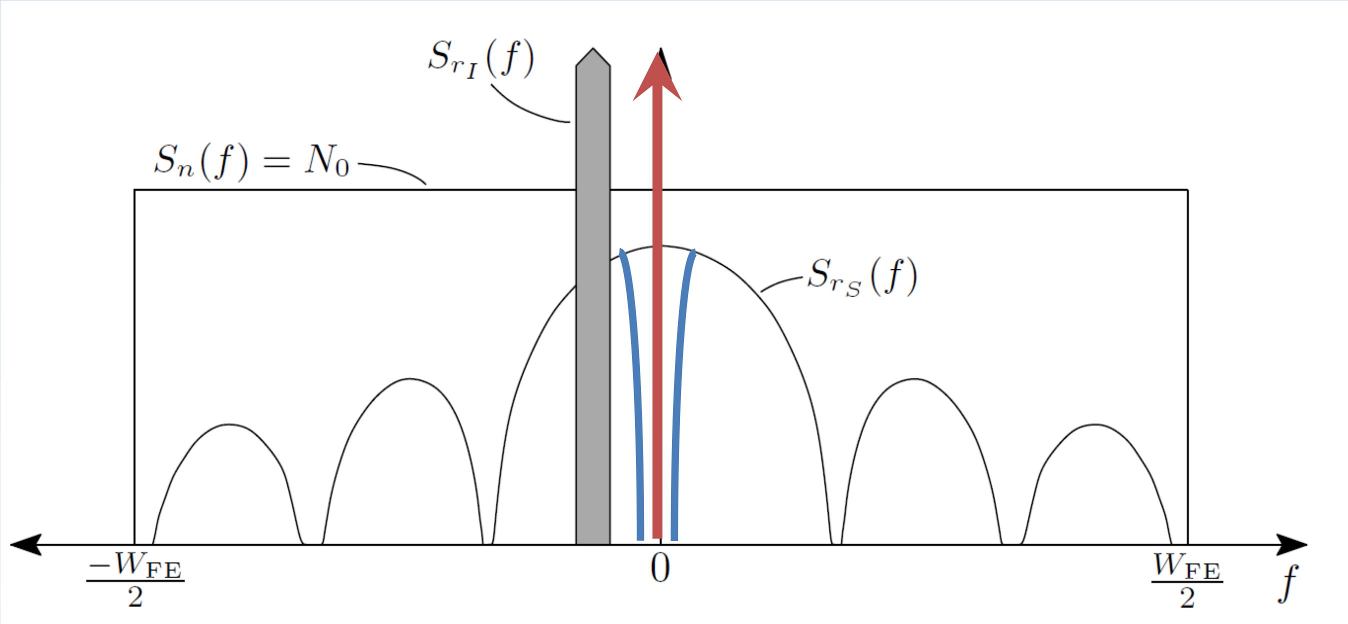


Q: Then why isn't the jammer in Syria using this most potent waveform?

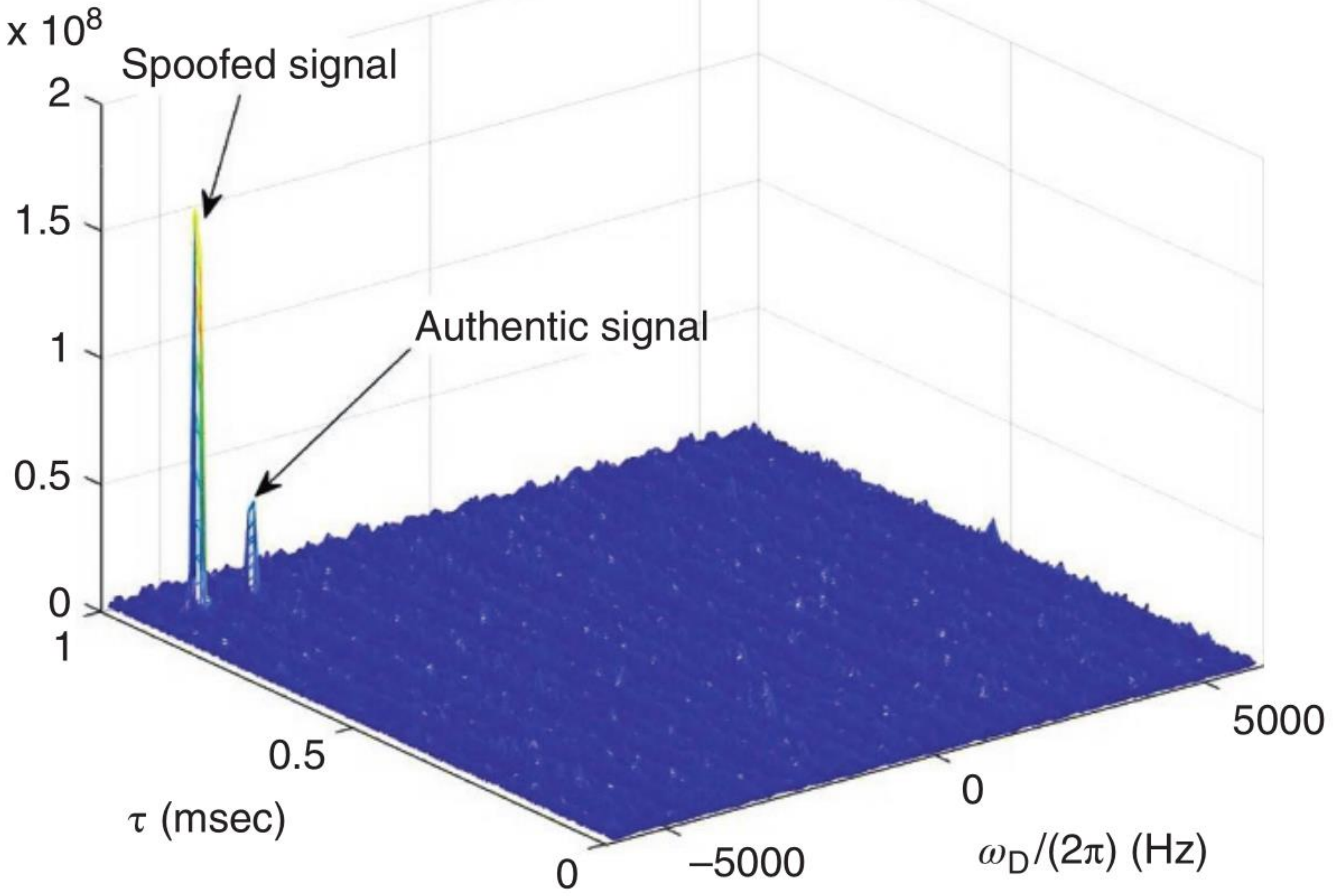


Q: Then why isn't the jammer in Syria using this most potent waveform?

A: It's too easy to defeat: a simple notch filter will do the trick.



To be both power-efficient and effective (hard to reject), the jamming signal has to produce high I_0 *but avoid being sparse in some domain* (e.g., time, frequency, code space, direction of arrival). A continuous matched-spectrum signal coming from multiple directions is both power-efficient and non-sparse (difficult to excise).



It takes very little interference power to present a cold-starting receiver with a conundrum: which peak does it choose?

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 matched-spectrum jammer at the same stand-off distance

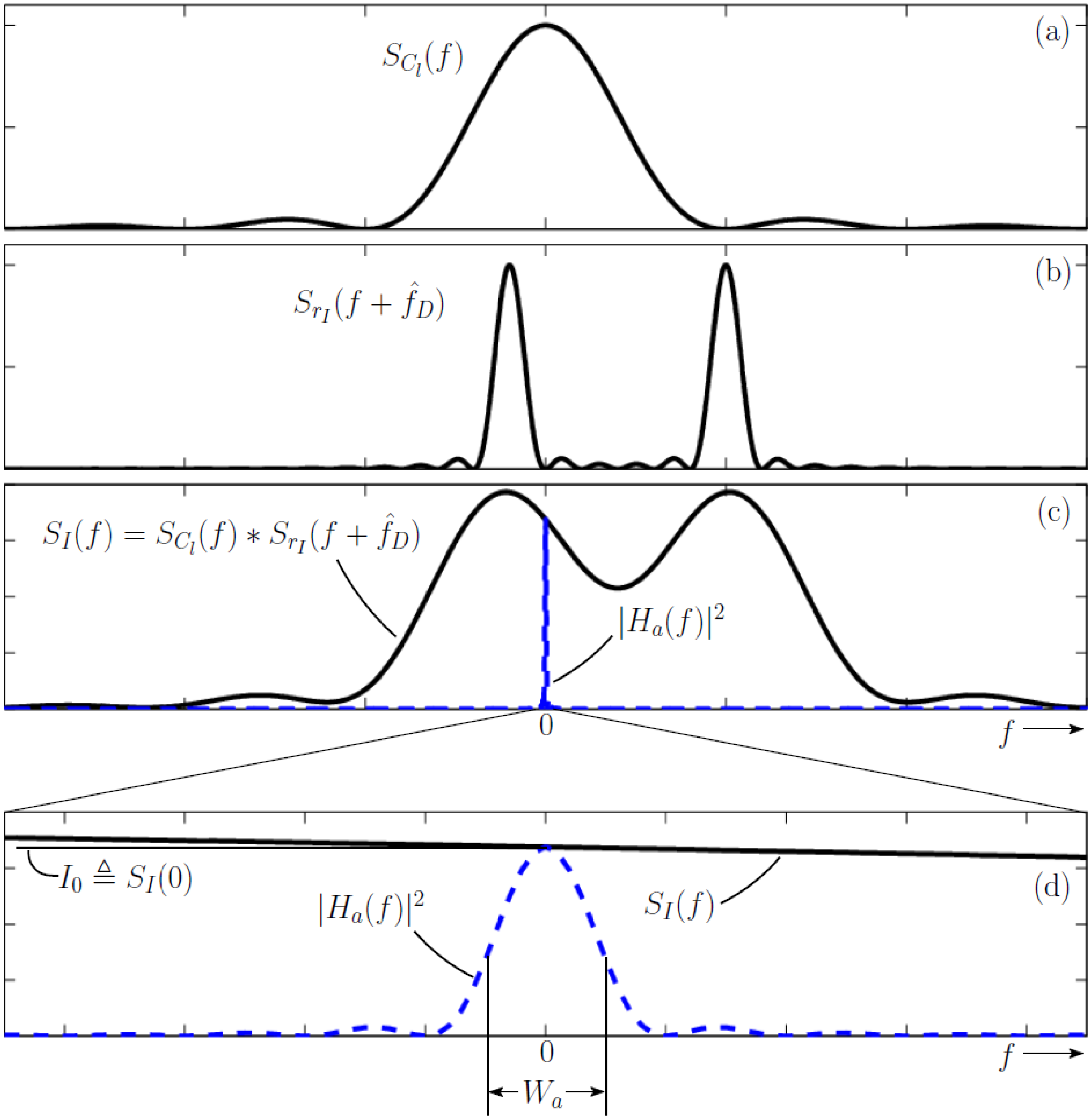
$$\frac{P_{\mathrm{I}}}{C} = -\left[\eta + 10\log_{10}\left(\frac{2T_{\mathrm{C}}}{3}\right)\right]$$

For a typical CINR acquisition threshold of $\eta = 30$ dB-Hz,
the received jamming-to-signal power ratio must be 31.8 dB to deny service. For DOS via spoofing it need only be 0 dB.

Q: What desired-signal spreading code is most effective for resisting interference? In other words, what S_{C_l} minimizes I_0?

$$I_0 := \int_{-W_{\mathrm{FE}}/2}^{W_{\mathrm{FE}}/2} S_{r_I}(f) S_{C_l}(f)\, df$$

A: The wider the better. M-Code BOC(10,5) is an excellent example.



Q: How do we build a resilient PNT box?

Q: First, how do we authenticate GNSS signals?

There are many spoofing detection and mitigation techniques. None is perfect. The practical objective is to price your adversary out of the game.

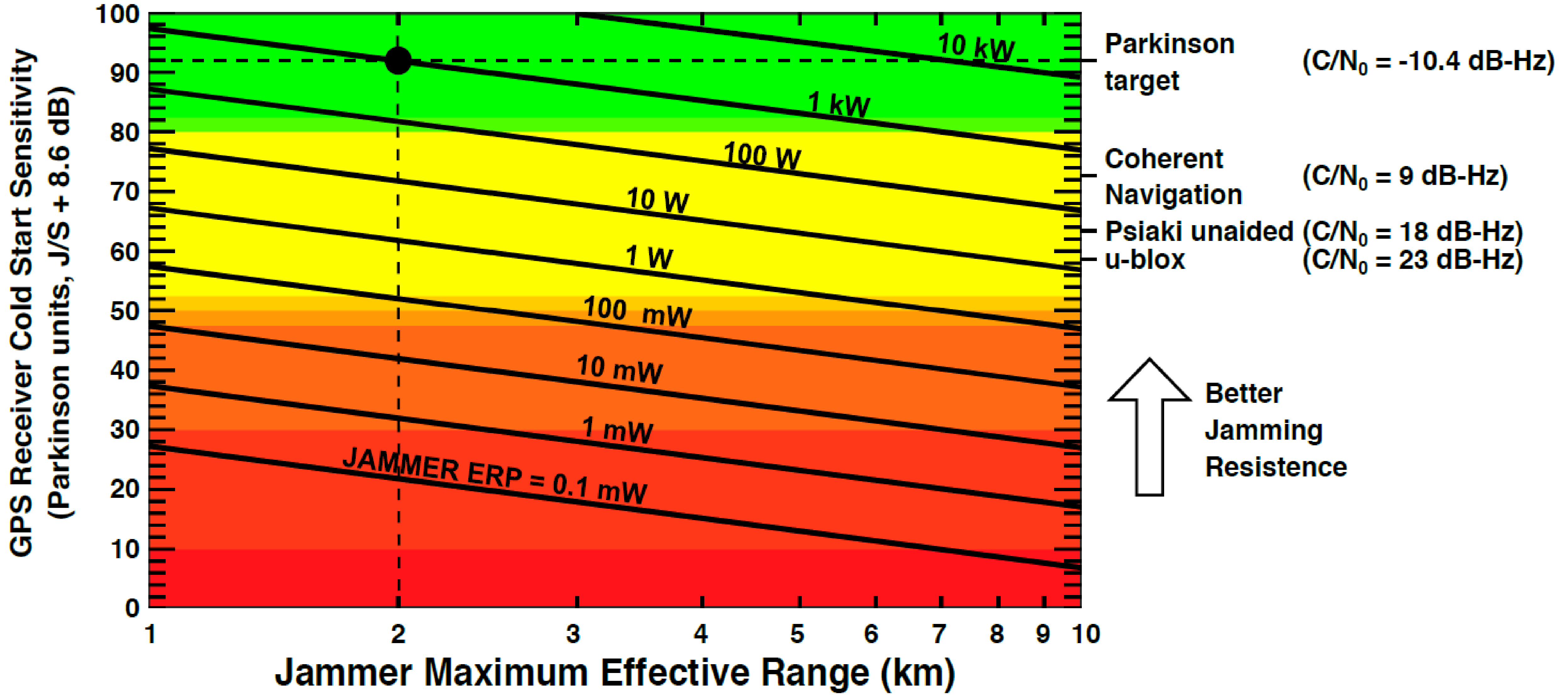
Psiaki, Mark L., and Todd E. Humphreys. “GNSS spoofing and detection.” *Proceedings of the IEEE* 104.6 (2016): 1258-1270.

TABLE I: Cost-Ranked Matrix of GNSS Spoofing Attack and Detection Techniques

Detection Techniques	Attack Techniques A1	A2	A3	A4	A5	A6	A7	A8	A9	A10	A11	A12	A13
D1	X	X	X	X	X	X	X	X	X	X	X	X	X
D2	∼	✓	X	X	∼	X	X	X	X	X	∼	X	X
D3	∼	∼	∼	∼	∼	X	X	∼	∼	∼	∼	X	X
D4	∼	✓	∼	∼	∼	∼	∼	∼	∼	∼	∼	∼	∼
D5	✓	✓	✓	✓	✓	∼	∼	✓	✓	✓	✓	∼	∼
D6	X	✓	✓	X	X	✓	X	✓	✓	X	X	✓	X
D7	X	✓	✓	∼	X	✓	∼	✓	✓	∼	X	✓	∼
D8	X	✓	✓	✓	X	✓	✓	✓	✓	✓	X	✓	✓
D9	∼	✓	✓	✓	∼	✓	✓	✓	✓	✓	∼	✓	✓
D10	✓	✓	✓	✓	✓	✓	✓	✓	∼	∼	∼	∼	∼
D11	✓	✓	✓	✓	✓	✓	✓	X	∼	∼	∼	∼	∼
D12	X	✓	✓	✓	X	✓	✓	✓	✓	✓	X	✓	✓
D13	X	✓	✓	✓	X	✓	✓	✓	✓	✓	X	✓	✓

	Attack Techniques Key		Detection Techniques Key
A1	Meaconing, single RX ant., single TX ant.	D1	Pseudorange-based RAIM
A2	Open-loop signal simulator	D2	Observables and RPM
A3	RX/SP, single TX ant., no SCER	D3	Correlation fcn. distortion monitoring
A4	RX/SP, single TX ant., SCER	D4	Drift monitoring (clock offset, IMU/position)
A5	Meaconing, multi. RX ants., single TX ant.	D5	Observables, RPM, distortion, and drift monitoring
A6	Nulling RX/SP, single TX ant., no SCER	D6	NMA*
A7	Nulling RX/SP, single TX ant., SCER	D7	NMA* and SCER detection
A8	RX/SP, single TX ant., sensing of victim ant. motion	D8	Asymmetric-key SSSC*
A9	RX/SP, mult. TX ants., no SCER	D9	NMA*, SCER detection, RPM, and drift monitoring
A10	RX/SP, mult. TX ants., SCER	D10	Multiple RX antennas
A11	Meaconing, multi. RX ants., multi. TX ants.	D11	Moving RX antenna
A12	Nulling RX/SP, mult. TX ants., no SCER	D12	Dual-RX correlation of P(Y) or M codes
A13	Nulling RX/SP, mult. TX ants., SCER	D13	Symmetric-key SSSC* [e.g., P(Y) equiv.]

Q: Next, how do we prevent denial of PNT?



PTA: By (1) deep coupling with inertial sensors, and (2) multi-element antennas we can toughen GNSS receivers enough to withstand 1 kW wideband Gaussian jammer at a distance of 2 km.

Robust, precise, high-integrity PNT for self-driving cars

University of Texas Sensorium

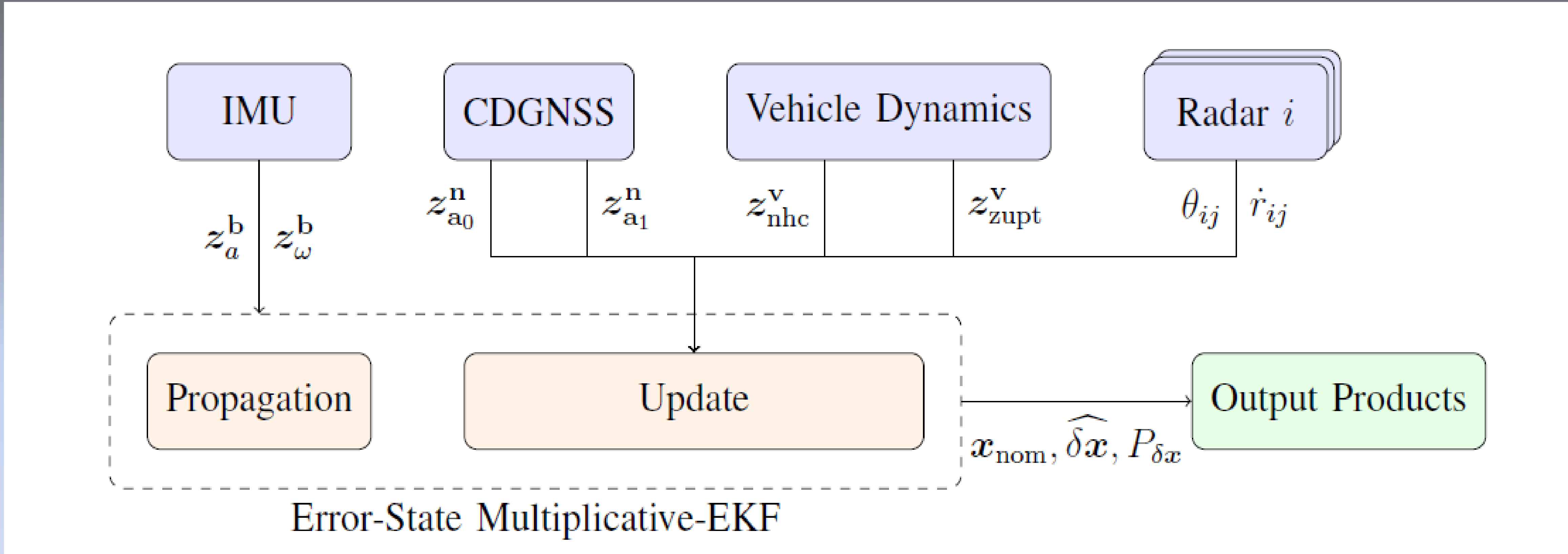
Emphasis on high-integrity PNT: Precise dual-antenna GNSS, three radar units, stereo cameras, inertial sensing, stable internal clock, LTE comms.

Ground Truth:

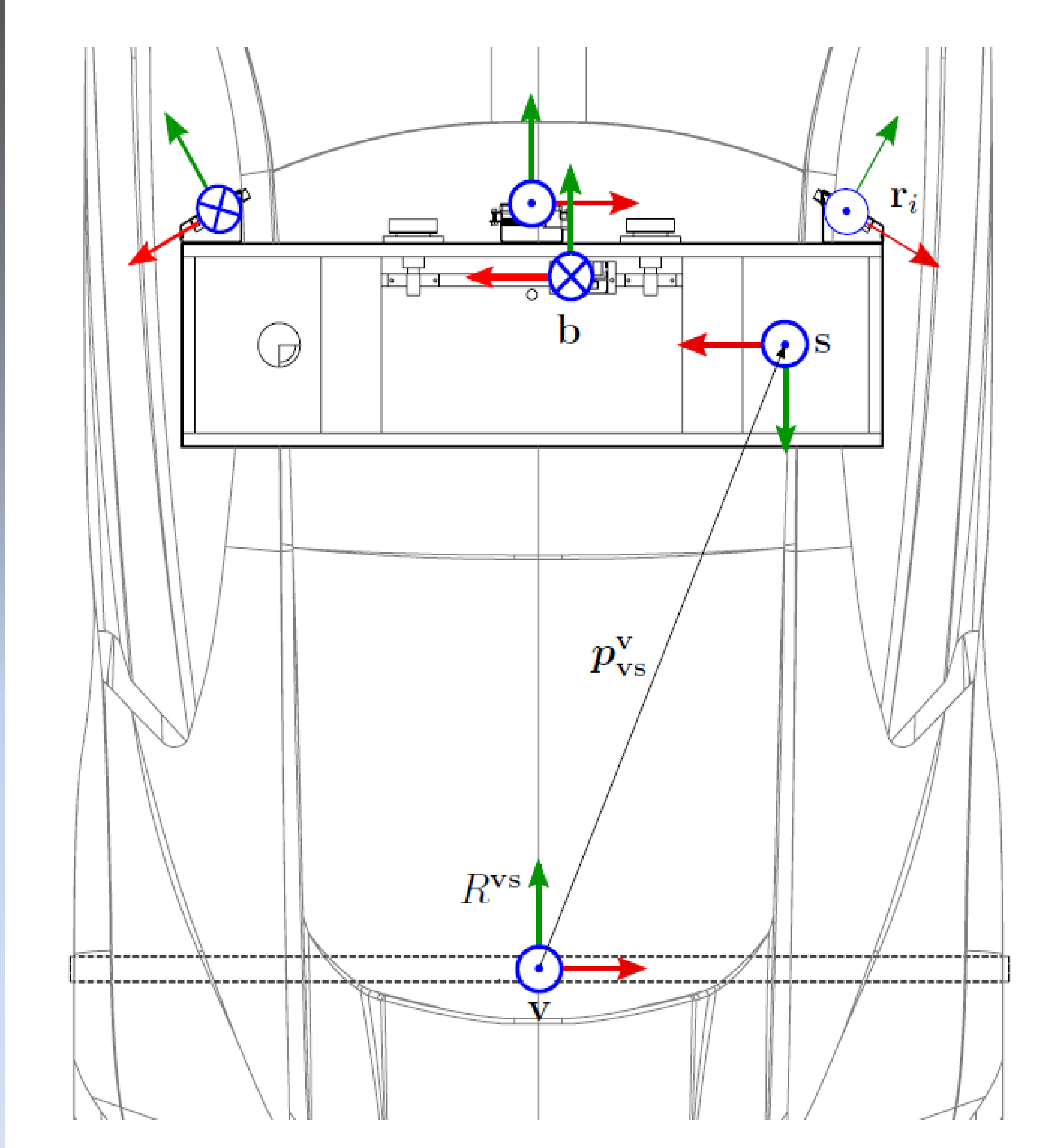
Forward-backward smoothed solution from iXblue ATLANS-C connected to the test antenna

The ATLANS-C “smartly” couples a tactical-grade IMU with a Septentrio RTK receiver

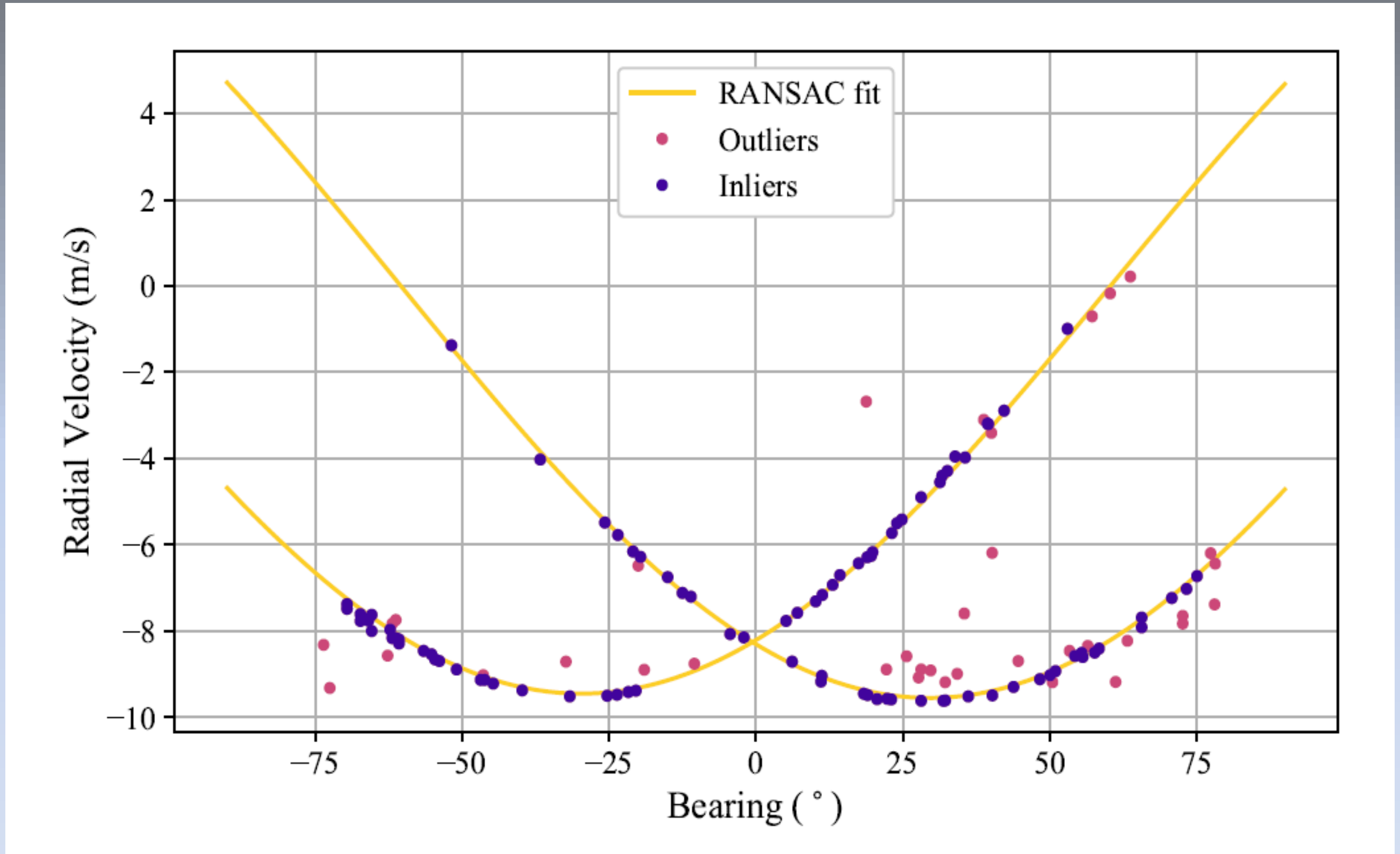
1-sigma reported uncertainty ranged from 2cm to 20cm

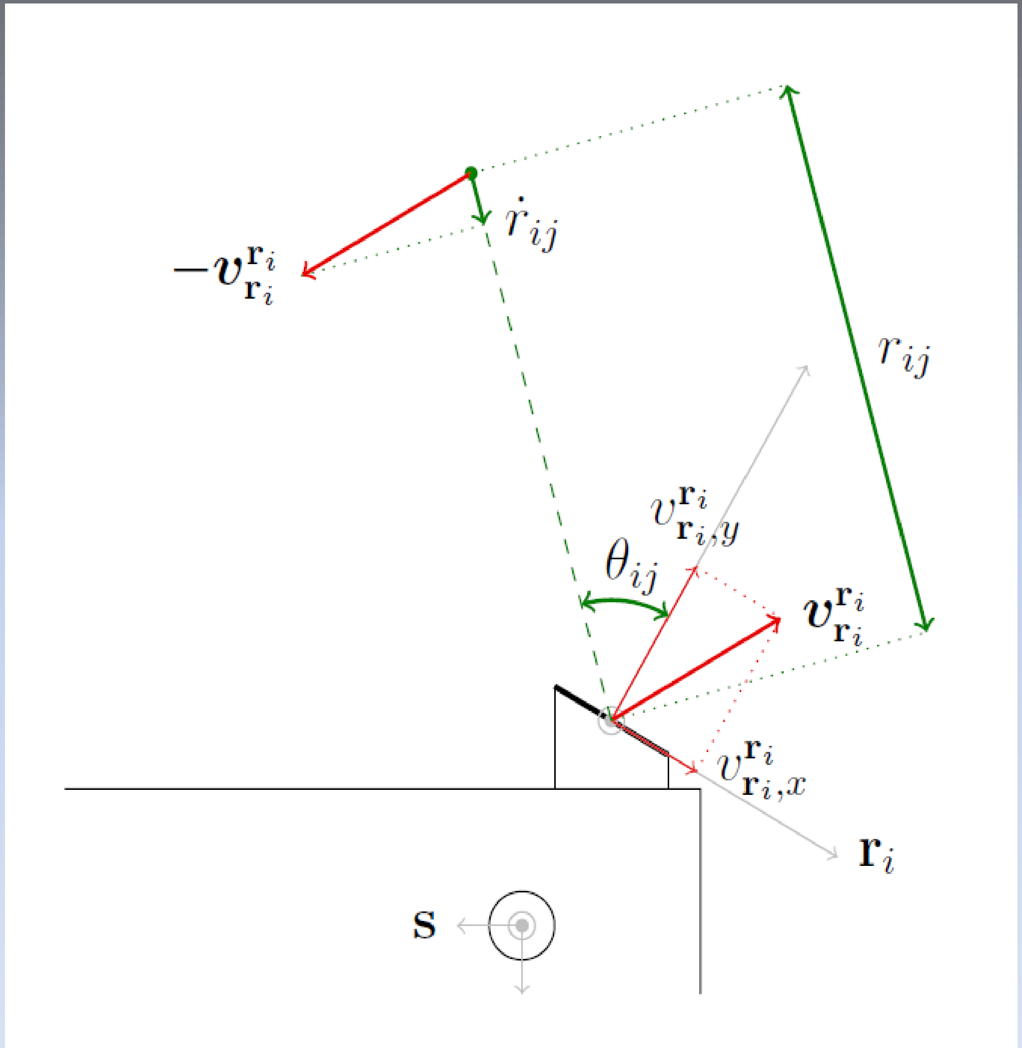


CDGNSS (when available), vehicle dynamics, and radar are fused to constrain drift of IMU

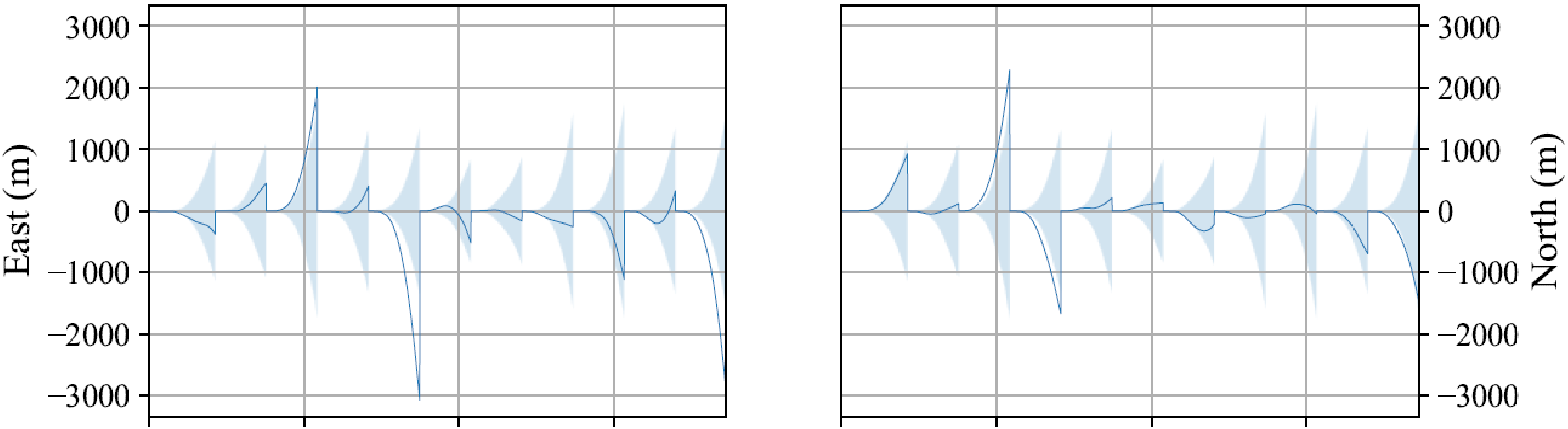


Must determine vehicle's center of rotation in order to apply zero-sideslip constraint

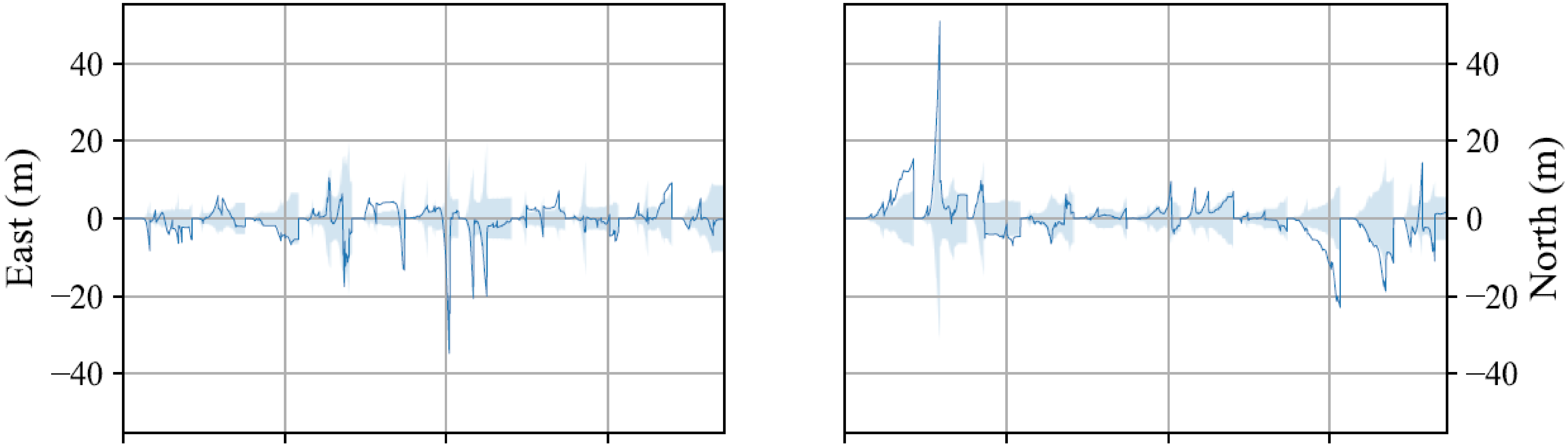




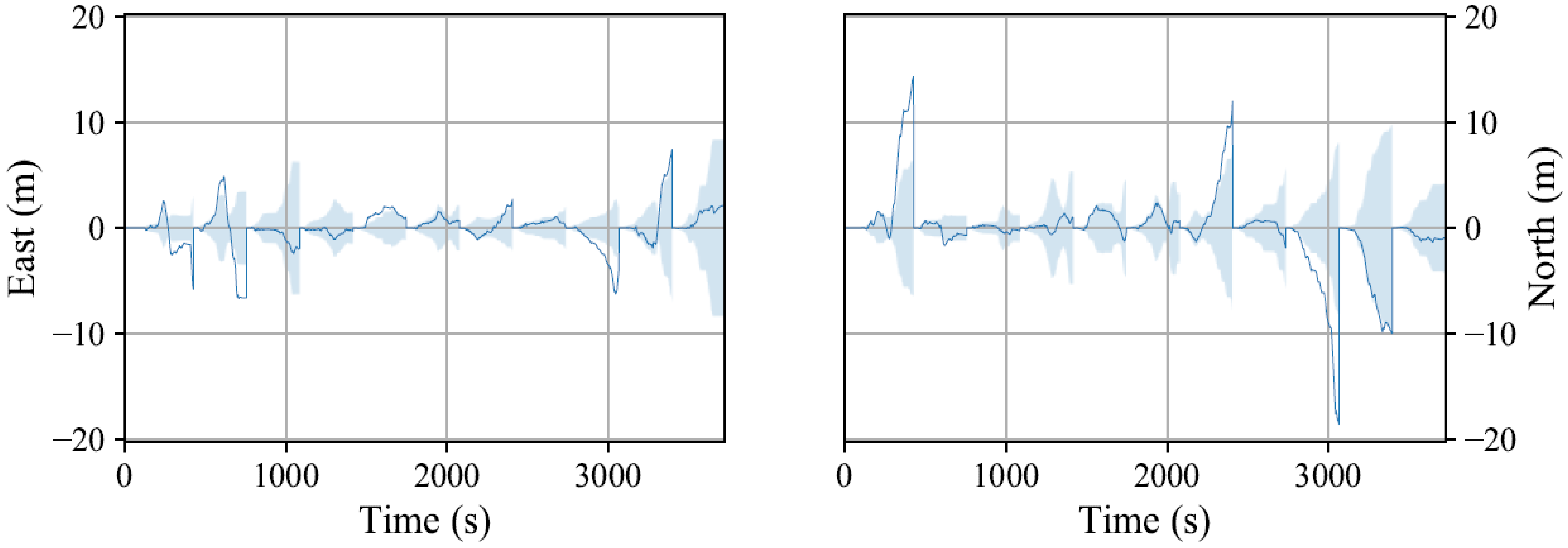
Must model and calibrate radar sensors



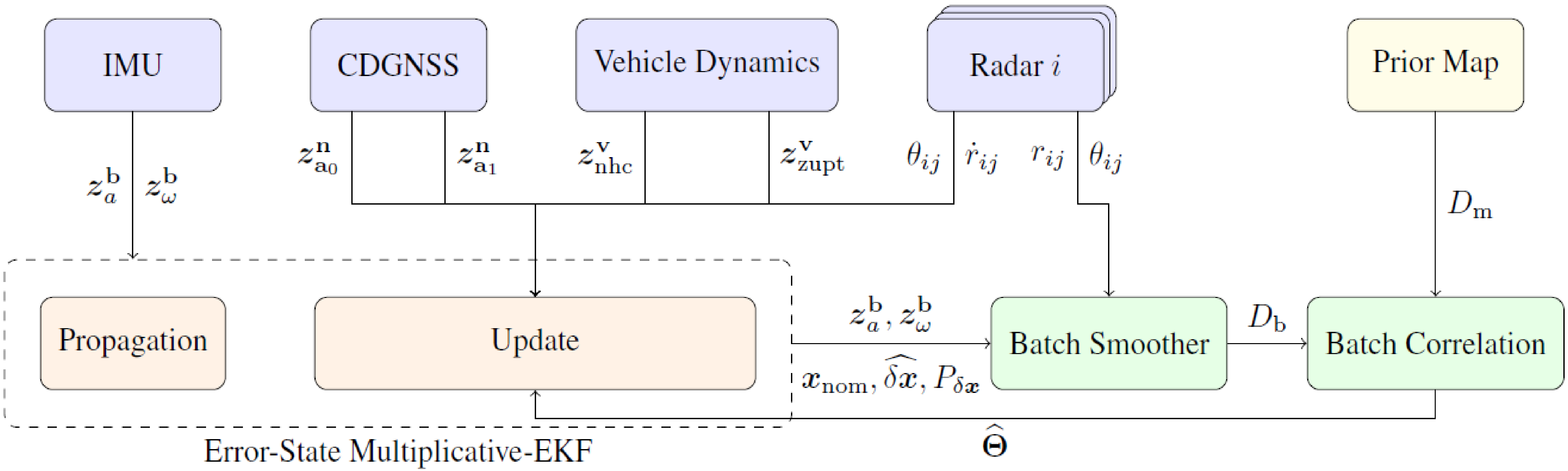
Periodic 5-minute GNSS outages:
High-end MEMS IMU drifts up to 2km



Now with vehicle motion model constraints (zero sideslip, ZUPD).
High-end MEMS IMU drifts less than 40 meters.

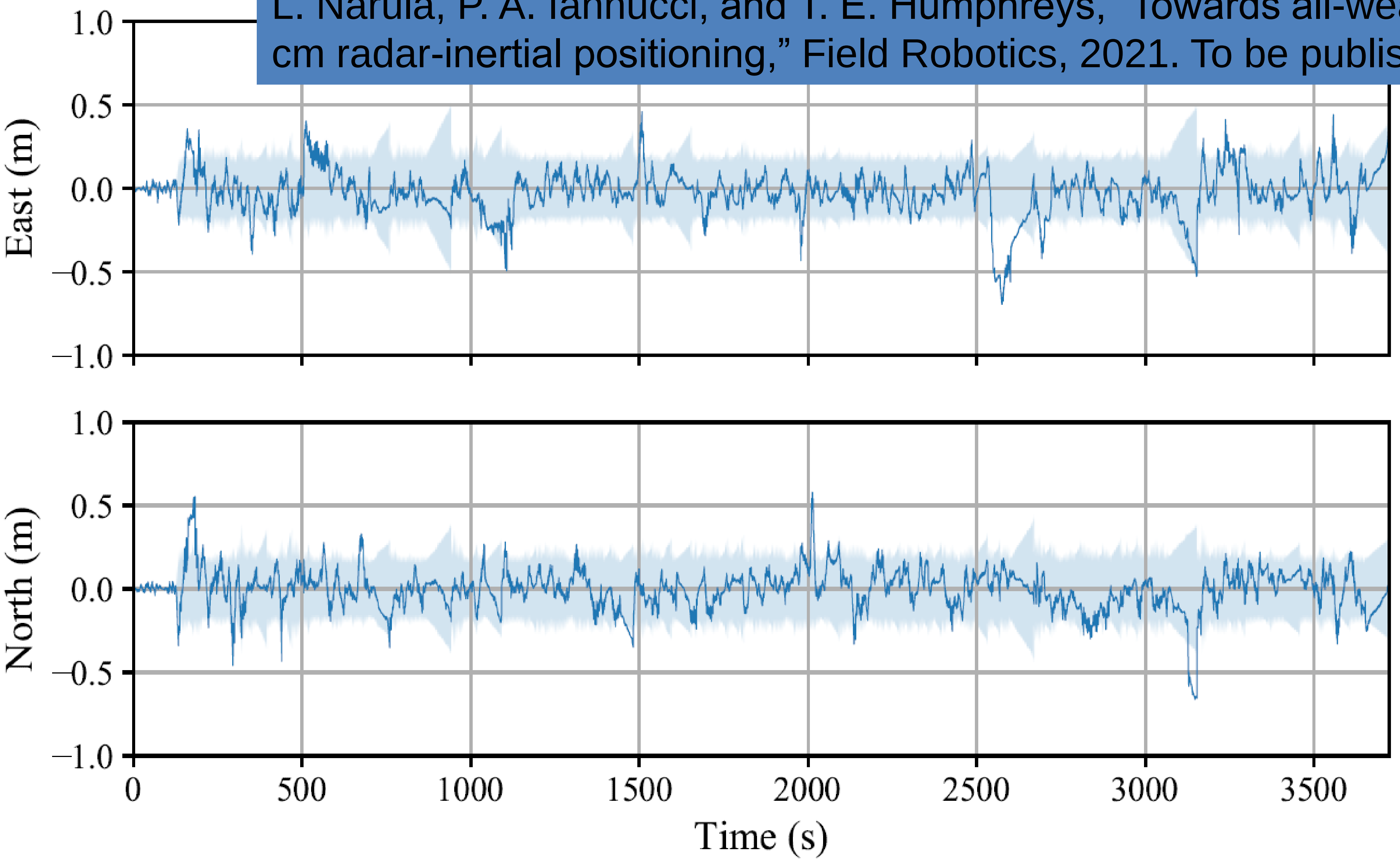


Additionally with radar range rate constraints (no prior map).
High-end MEMS IMU drifts less than 20 meters.



Further constrain with a prior radar map

L. Narula, P. A. Iannucci, and T. E. Humphreys, “Towards all-weather sub-50-cm radar-inertial positioning,” Field Robotics, 2021. To be published.



A prior radar map enables 60-minute GNSS-denied vehicle positioning to better than 0.5 meters.

T. E. Humphreys, Interference, pp. 469-503. Springer International Publishing, 2017

Psiaki, Mark L., and Todd E. Humphreys. “GNSS spoofing and detection.” *Proceedings of the IEEE* 104.6 (2016): 1258-1270.

M. L. Psiaki and T. E. Humphreys, Position, Navigation, and Timing Technologies in the 21st Century: Integrated Satellite Navigation, Sensor Systems, and Civil Applications, vol. 1, ch. Civilian GNSS Spoong, Detection, and Recovery, pp. 655{680. Wiley-IEEE, 2020

L. Scott, Position, Navigation, and Timing Technologies in the 21st Century: Integrated Satellite Navigation, Sensor Systems, and Civil Applications, vol. 1, ch. Interference: Origins, Effects, Mitigations, pp. 619-654. Wiley-IEEE, 2020

L. Narula, P. A. Iannucci, and T. E. Humphreys, “Towards all-weather sub-50-cm radar-inertial positioning,” Field Robotics, 2021. To be published.

M. J. Murrian, L. Narula, P. A. Iannucci, S. Budzien, B. W. O'Hanlon, S. P. Powell, and T. E. Humphreys, “First results from three years of GNSS interference monitoring from low Earth orbit,” Navigation, Journal of the Institute of Navigation, 2021. Submitted for review.

T. E. Humphreys, M. J. Murrian, and L. Narula, “Deep-urban unaided precise global navigation satellite system vehicle positioning,” IEEE Intelligent Transportation Systems Magazine, vol. 12, no. 3, pp. 109-122, 2020

THE UNIVERSITY OF TEXAS AT AUSTIN

RADIONAVIGATION LABORATORY