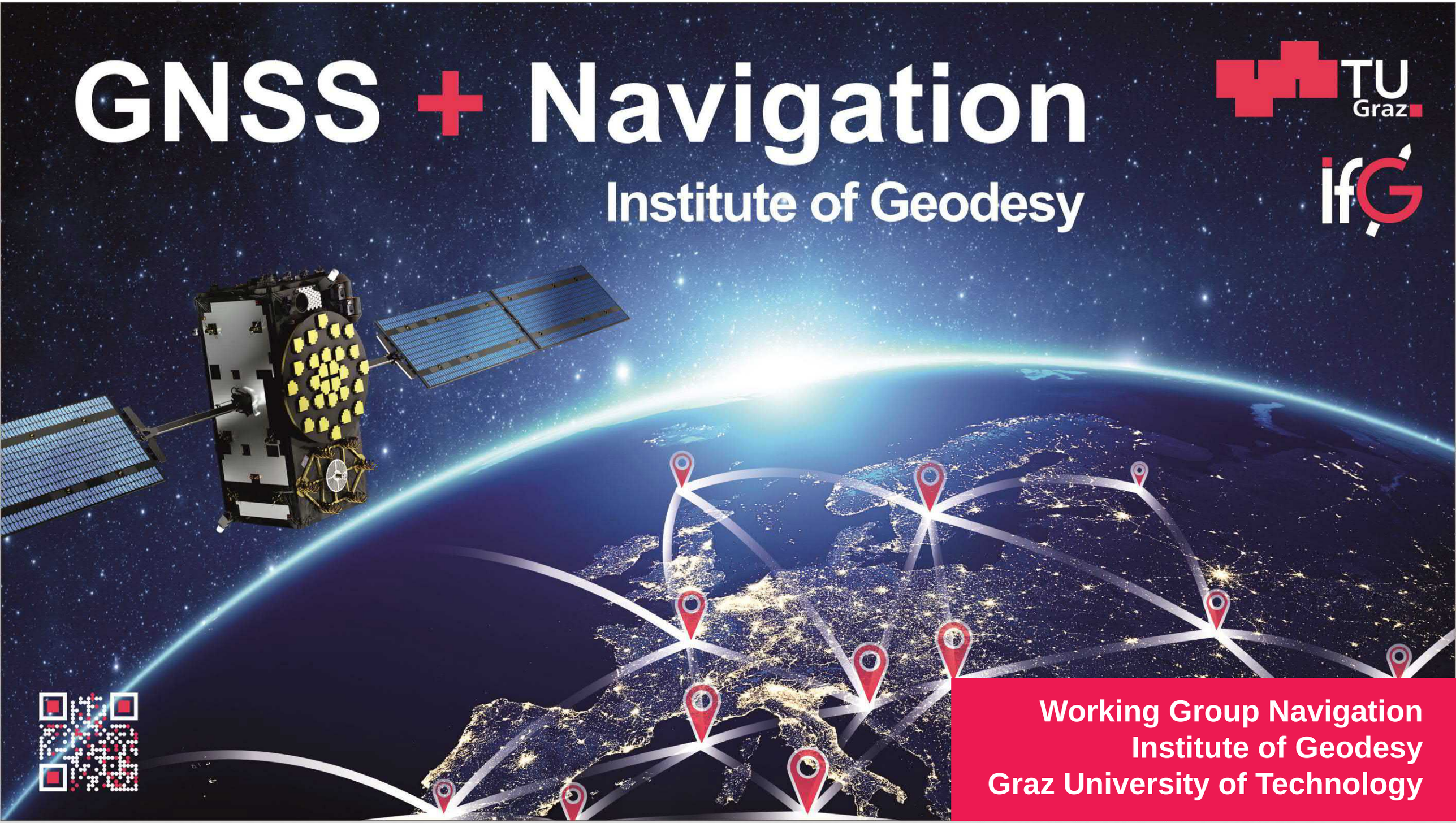
GNSS + Navigation

Institute of Geodesy



Working Group Navigation
Institute of Geodesy
Graz University of Technology

WISSEN
TECHNIK
LEIDENSCHAFT

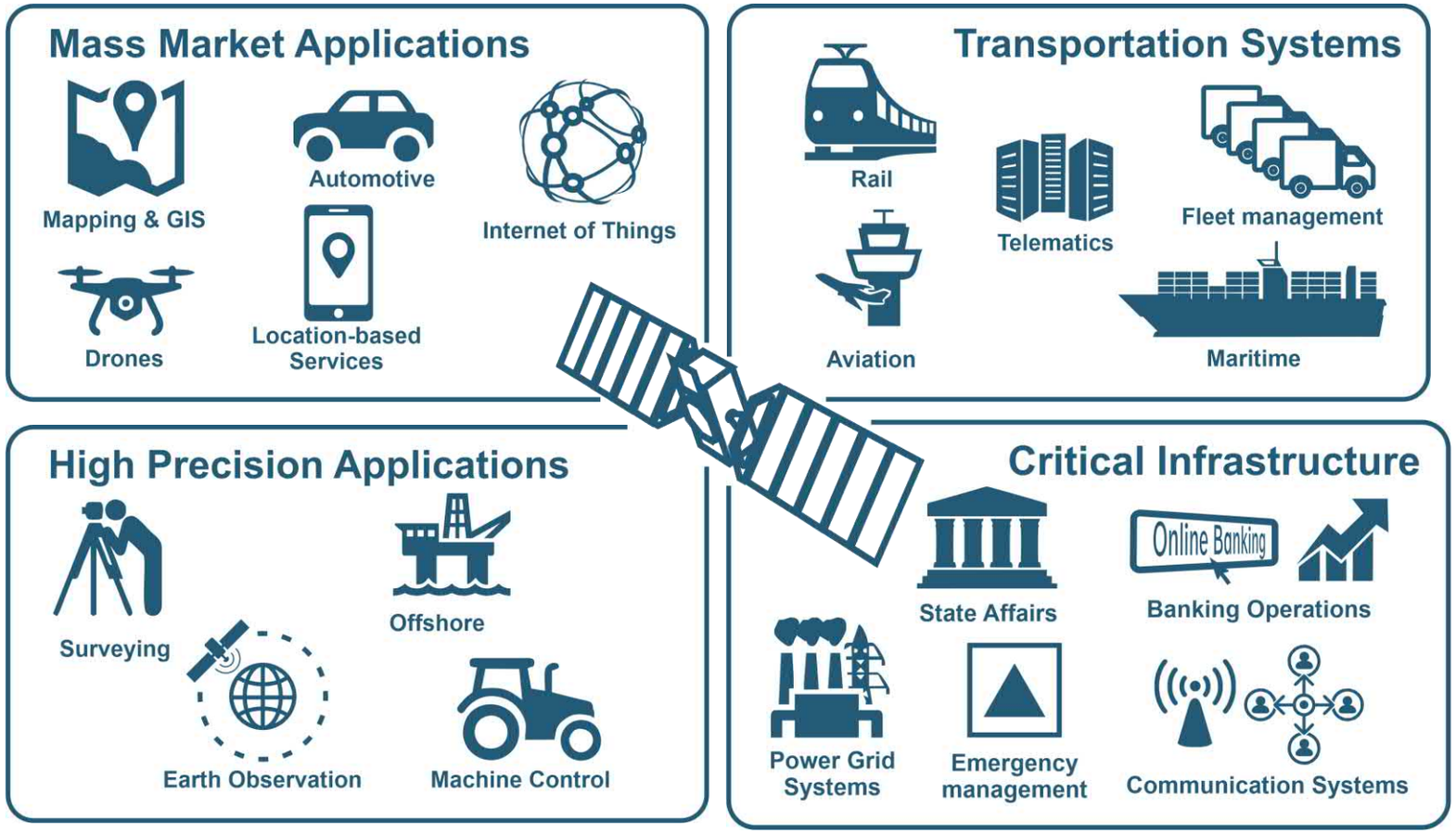
What makes GNSS vulnerable?

GNSS Under Attack Workshop

Univ.-Prof. Dr. Philipp Berglez

5 February 2026

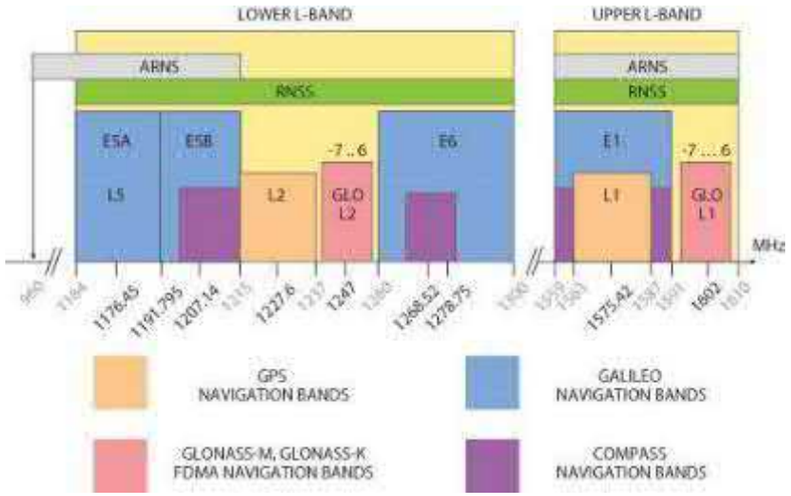
GNSS Applications



Even small disruptions can cause severe errors!

GNSS frequencies

- Frequency allocation strictly regulated by International Telecommunications Union (ITU)
- GNSS frequency bands



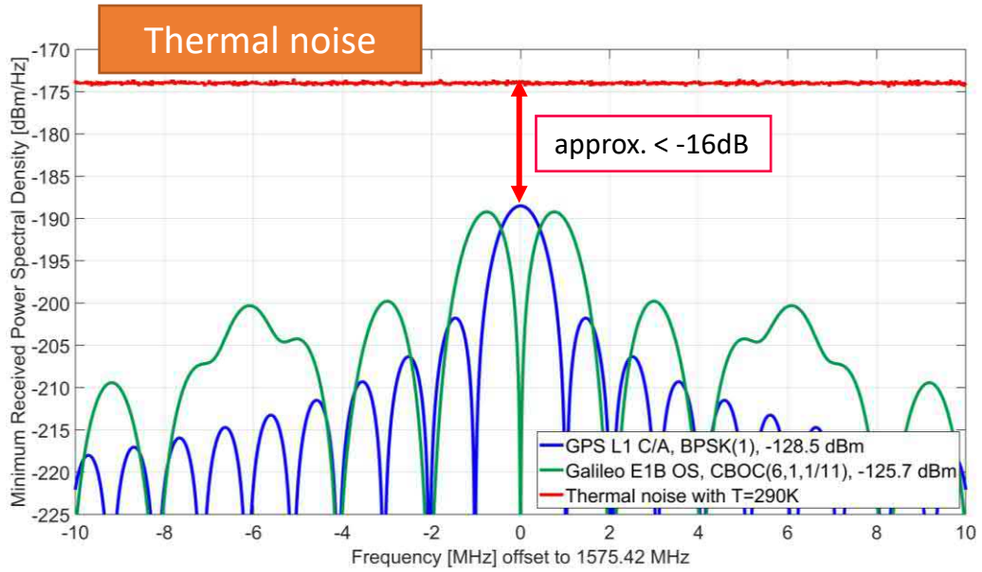
MicrowaveJournal.com May 2012

- Interference can be described as the effect of energy change due to the superposition of electromagnetic waves
- ‘THE VOLPE REPORT’ → 29th August 2001

Why are GNSS signals vulnerable?

- GNSS are highly complex systems

- GNSS signals received on earth are very weak
  - Approx. -130 dBm received signal power
  - Power level is equivalent to that of a 30 Watt light bulb after traveling more than 20,000 km
  - GNSS bands dominated by white noise, SNR typical -15 … --35 dB



-16dB → Factor ≈ 1/40

- Signal design dates back to the 70s/80s

- GNSS signals extremely susceptible to all types of interference

Classification of interference

- Unintentional interference
  - Natural interference
  - Intra-system interference (e.g., Galileo SV1 ⇔ SV2)
  - Inter-system interference (e.g., Galileo ⇔ GPS)
  - Self-interference: e.g., inter-symbol interference; inter-modulation product
  - External interference (e.g. other known RF systems)

  Dealing with unintended interference is well known and poses less of a problem

- Intentional interference
  - Jamming
  - Spoofing
  - Meaconing

Intentional interference - Jamming

- Jamming's objective is denial of navigation service by masking GNSS signals with noise
  - Intentional transmission of RF energy to hinder a navigation service by drowning (masking) GNSS signals with noise
  - Objective to cause a receiver to lose tracking and impede signal reacquisition

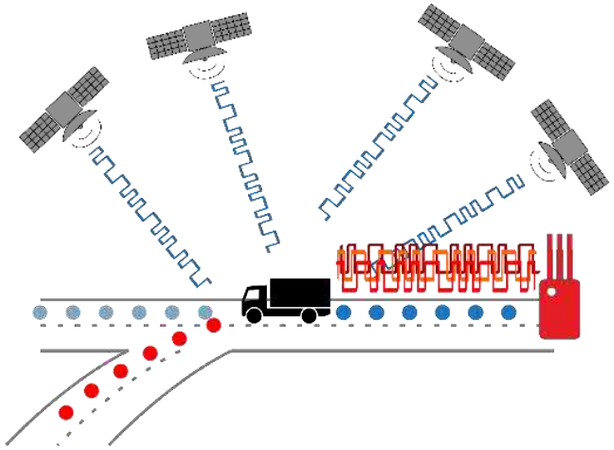
- Motivation / examples:
  - Turning off car anti-theft-systems
  - Bypassing pay-as-you-drive insurance
  - Withdrawing Fleet Management System
  - Protecting the privacy of parcel delivery agents from their employers
  - Protection of critical infrastructure
  - Electronic warfare
  - Etc.

Impact of jamming

- Decreased/degradation of signal strength and quality
  - Lower SNR and C/N0
  - Lower availability of observables
  - Longer acquisition time and longer time-to-first-fix
  - Loss of signal tracking
- Measurement quality
  - Increased noise within tracking loops → degradation of accuracy
  - Increased number of cycle slips
- PVT accuracy → Denial of service
- Damage the receiver hardware

Intentional interference - Spoofing

- Spoofing refers to the transmission of fraudulent GNSS-like signals, that force the victim receiver to compute erroneous positions.
  - Intentional transmission of a fake GNSS-like signal
  - Deliberate manipulation of PVT information in the receiver
  - Without disrupting operations



- Meaconing is the interception and rebroadcast of navigation signals
  - Multipath – environmental meaconing

How easy it is … → GNSS crop circles

P. Berglez (2024): Den GNSS-Kornkreisen auf der Spur. In Proceedings of the AHORN 2024 conference, Schladming, Austria, December 4 2024.

First reports of GNSS crop circles in 2019

MIT Technology Review

Featured Topics Newsletters Events Podcasts Sign in Subscribe

SMART CITIES

Ghost ships, cro
GPS mystery in

A sophisticated new electronic warfare
busiest port. But is it sand thieves or the

By Mark Harris

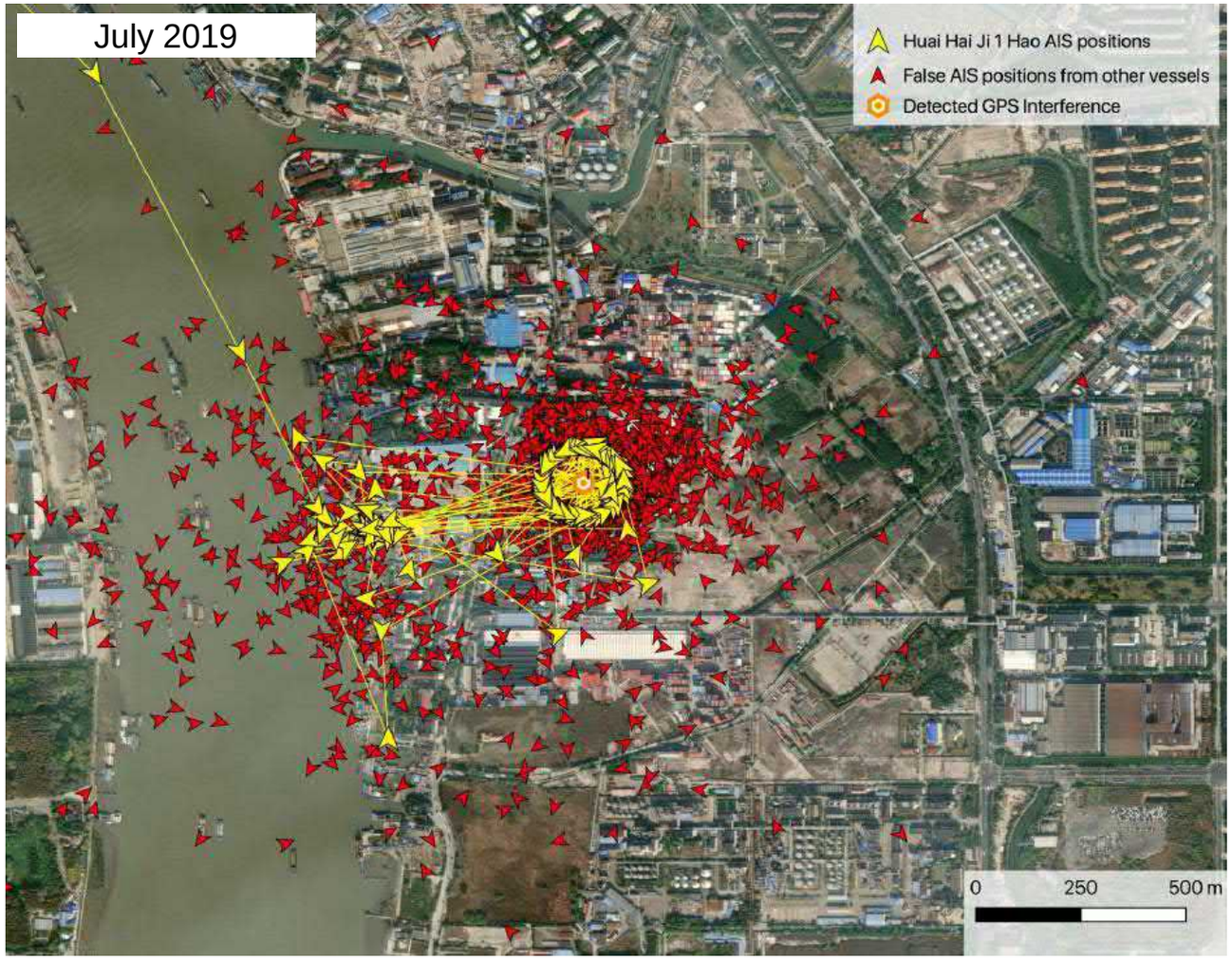
- Why?
- For what reason?
- For what purpose?

- An attempt at an explanation...

Ref : https://www.technologyreview.com/2019/11/15/131940/ghost-ships-crop-circles-and-soft-gold-a-gps-mystery-in-shanghai/

Ghost ships on the Huangpu River in Shanghai

- Huangpu River in Shanghai
- AIS (Automatic Identification System) ship positions

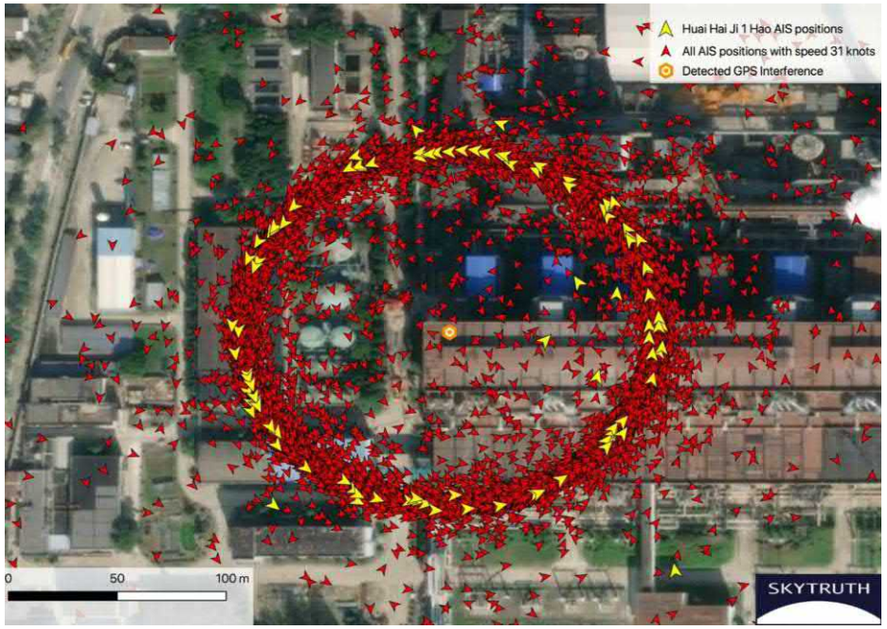


Ref.: https://www.marinetraffic.com

Ref.: Bergman B. (2022): Manipulation and GNSS Interference in Global AIS Ship Tracking Data. In Proceedings of Munich Satellite Navigation Summit 2022

A new dimension: GNSS circle spoofing

- Not only AIS data is affected, but also other GNSS devices (e.g. fitness trackers)
  - No ‘error’ with AIS

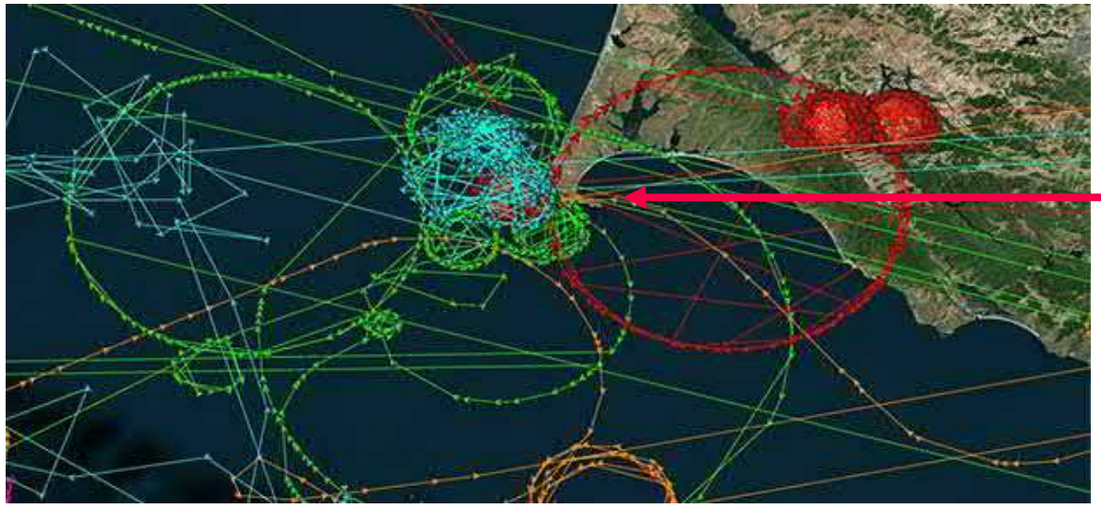


Ref.: Bergman B. (2022): Manipulation and GNSS Interference in Global AIS Ship Tracking Data. In Proceedings of Munich Satellite Navigation Summit 2022

Ref.: C4ADS

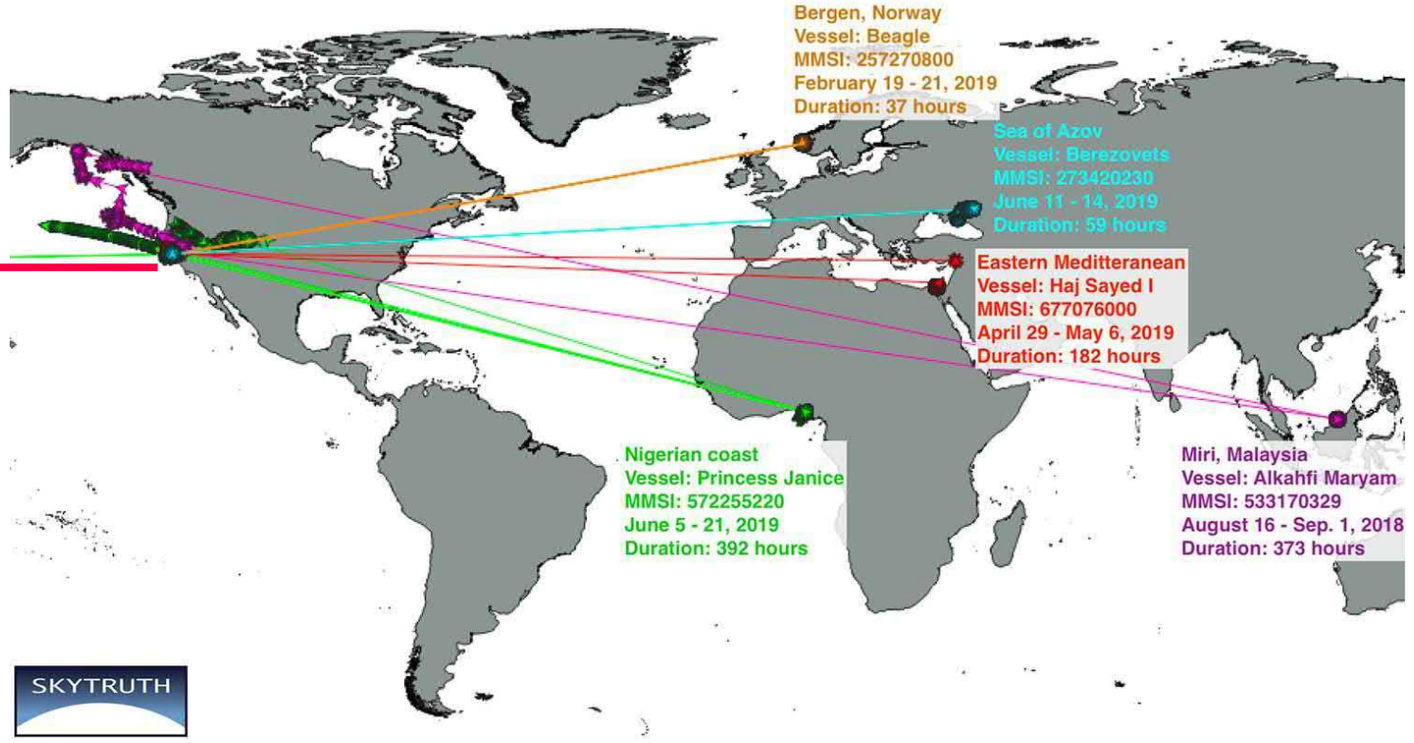
Further incidents in the maritime sector

- GNSS circle spoofing has been observed in various locations.



Point Reyes, USA

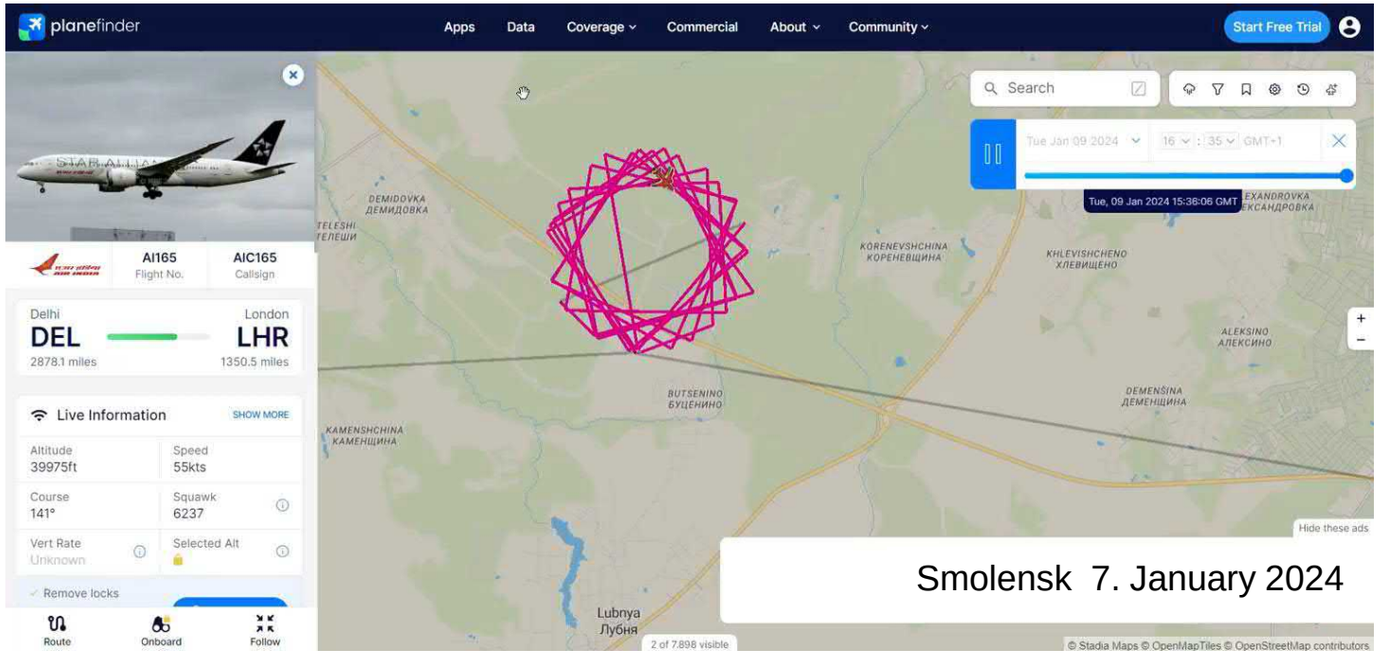
N 38° 3‘ 52“
W 123° 6‘ 13“

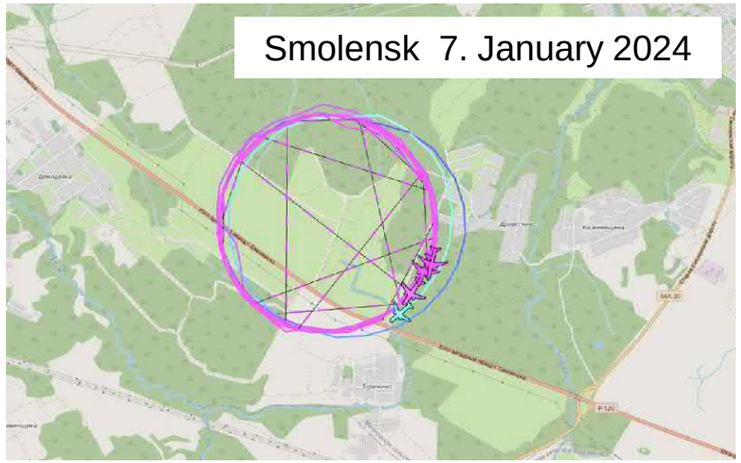


Ref.: www.gpsworld.com

Further GNSS circle spoofing incidents

- Aircraft, ships and GNSS trackers



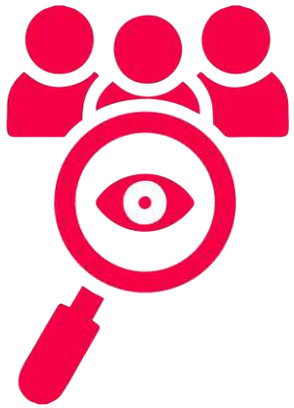


Ref.: https://www.gpsworld.com/gps-circle-spoofing-discovered-in-iran/

Ref.: https://rntfnd.org/2024/01/07/circle-spoofing-comes-to-aviation-first-the-baltic-now-the-mediterranean/

Ref.: https://x.com/giammaiot2/status/1745153888469082571

Why? How come? What for?



- What stands out? – Initial observations
  - It is GNSS spoofing
  - Different locations and countries
  - No military facilities affected and no crisis areas. (at least no reports of this)
  - Impact on receivers whose information is publicly available
    - Result/effect easy to observe
  - Impact on single-frequency, single-system receivers (AIS, ADS-B, trackers) → GPS L1 C/A Signal
  - Circular trajectory
    - Radius between 150 and 500+ m
      - Shanghai 150 m
      - Smolensk 500m
      - Teheran 500 m
      - Point Reyes 500 m – 10 km

GNSS spoofing basics

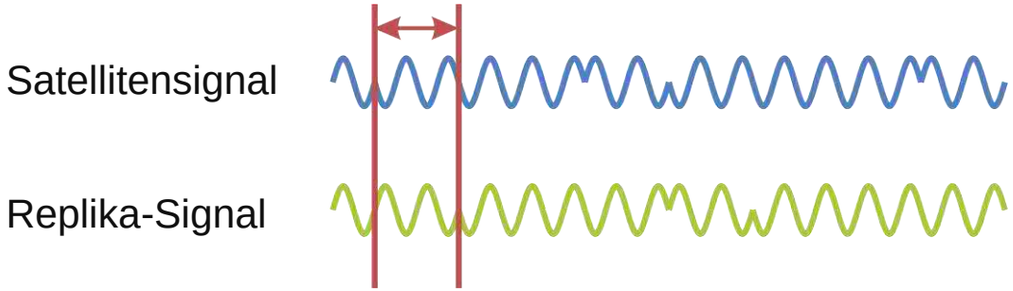
- Transmission of fake GNSS-like signals with the aim of generating a false position/time in the victim's receiver without disrupting operation.

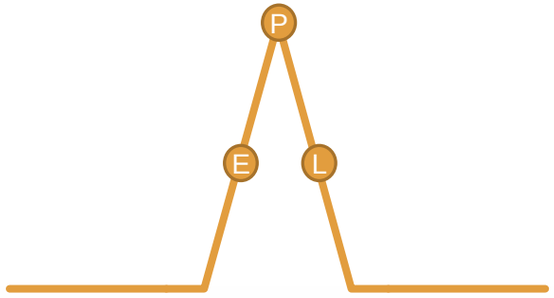
- Successful spoofing requires
  - Taking over the victim's receiver and gaining control of its movement
  - Synchronisation with the GNSS signal
  - Knowledge of the satellite positions

- Requirements
  - Ability to generate spoofing signals → signal simulator
  - Ability to transmit spoofing signals → RF transmitter

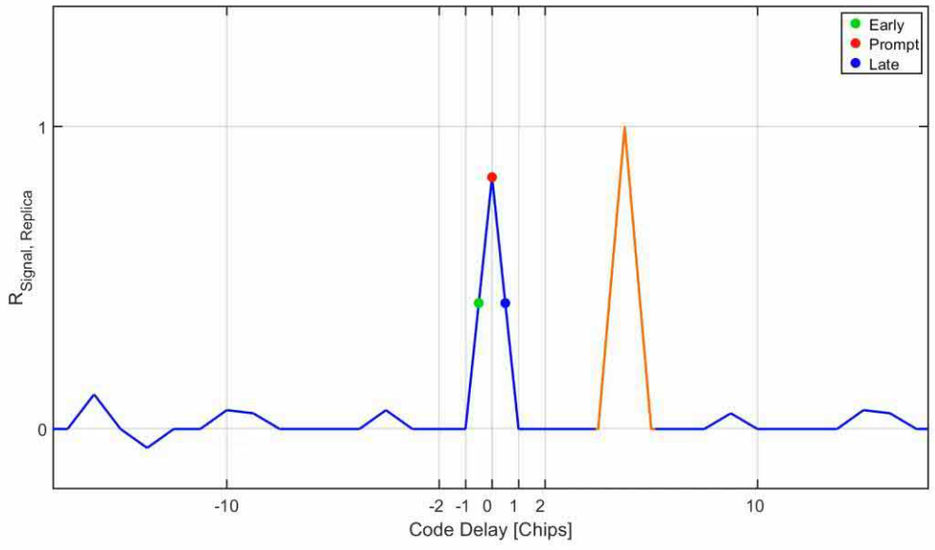
Spoofing Take Over

- The basic principle of GNSS signal processing is based on signal correlation.



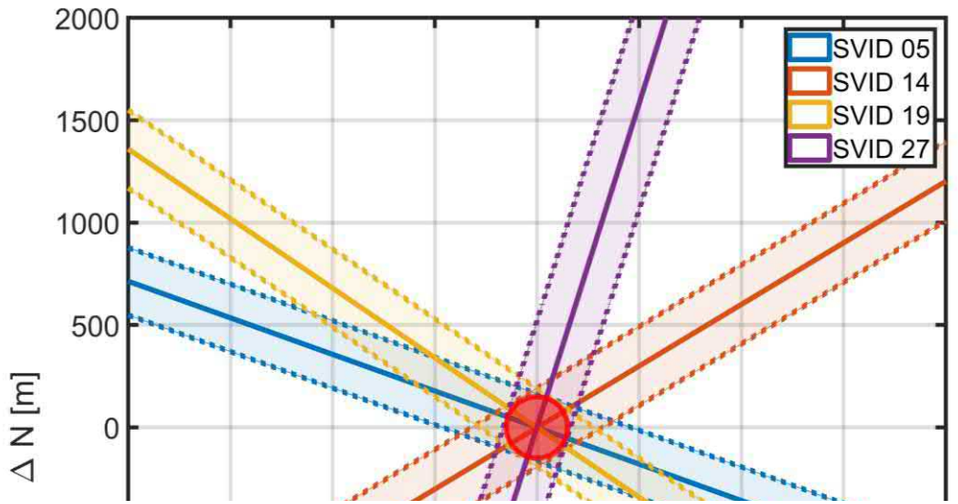


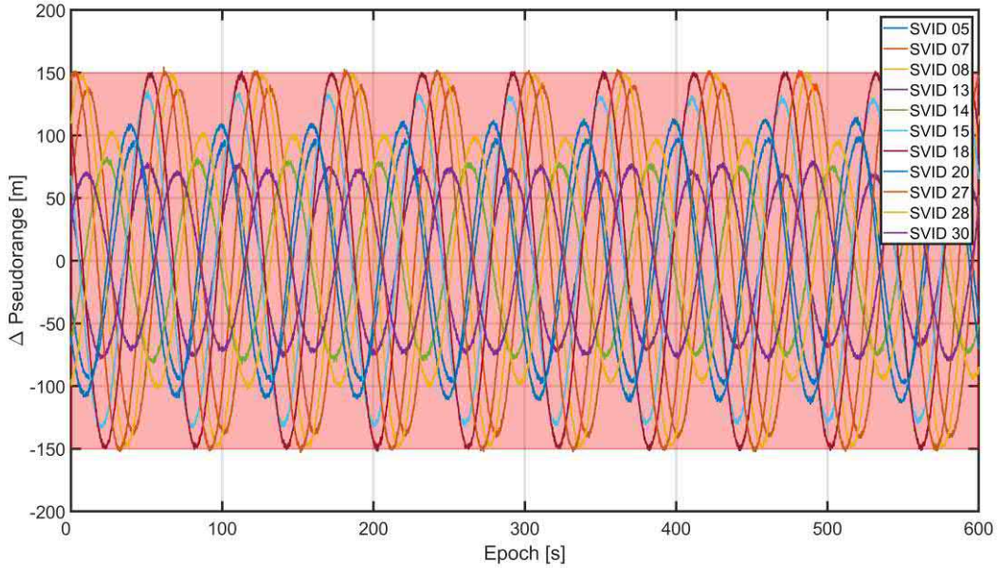
- Spoofing signal must ‘take over’ the correlators (E-P-L) of the receiver
  - Synchronisation with GNSS signal
  - Spoofing signal must be slightly stronger
  - Depending on GNSS signal component and tracking architecture
    - Standard procedure GPS L1 C/A
      → ± ½ Code-Chip



Why a circular trajectory?

- Position determination based on trilateration
  - Intersection of spherical shells
- Intersection curves of the spherical shells with local horizontal plane are circles
- Take-over requires synchronisation of signals within ± ½ code chip
  - Circle with radius 150 m → ± ½ code chip
- In a circular trajectory, all pseudoranges are within ± 150 m (± ½ code chip) in relation to the authentic pseudorange



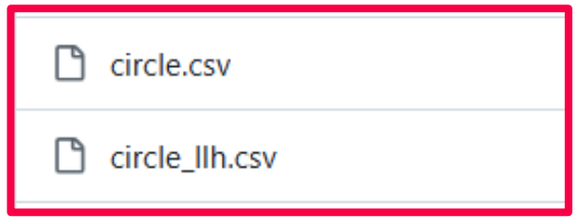


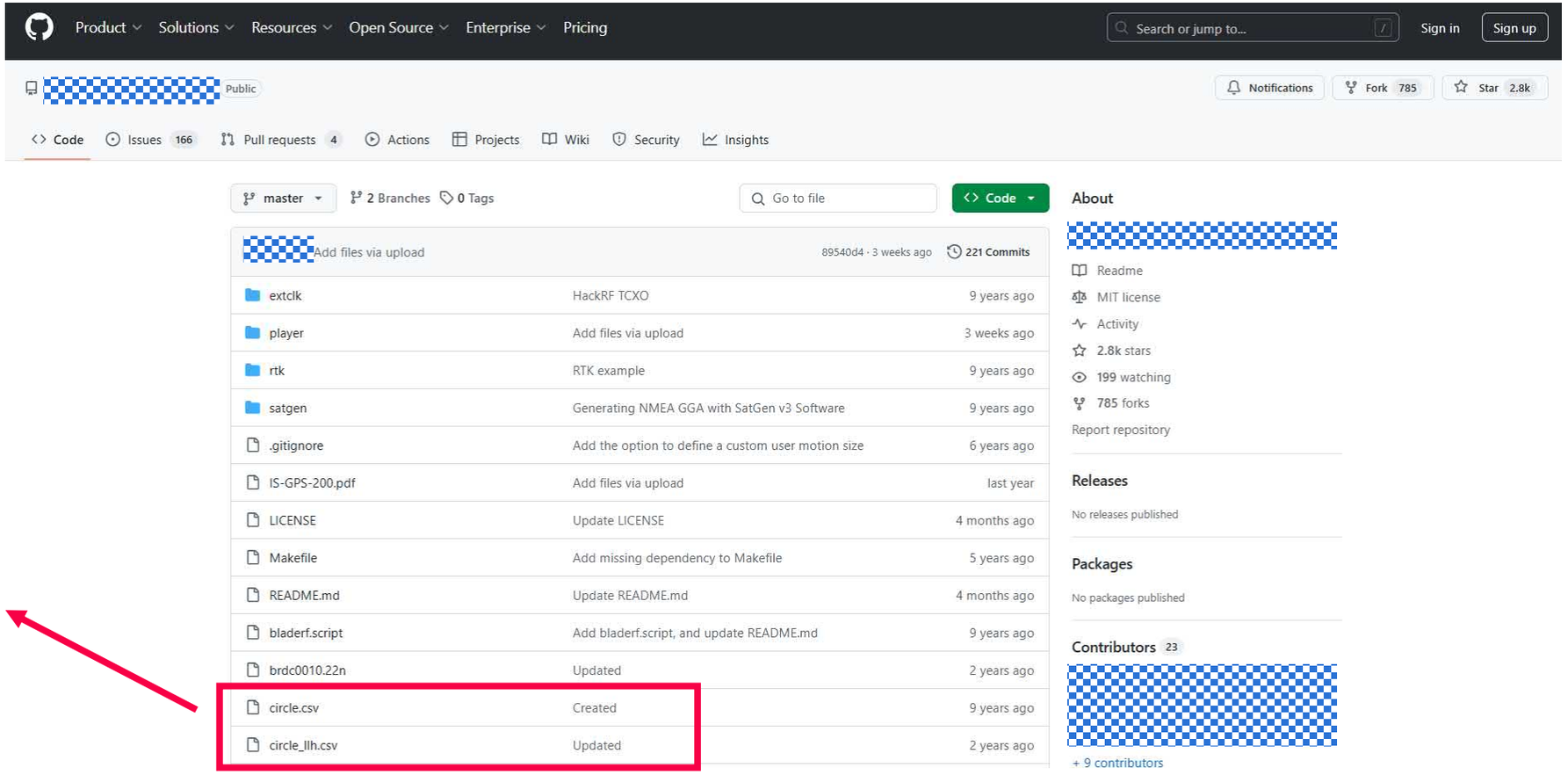
Where can you get a GNSS simulator/spoofer?

- Well-known manufacturers of simulators
- Manufacturers in the defence sector

Github – Software Simulator GPS L1 C/A

- Existing since 2015
  - C/C++ Code
  - GPS L1 C/A
  - Interface to RF transmitter
- File with trajectory
  - circle.csv

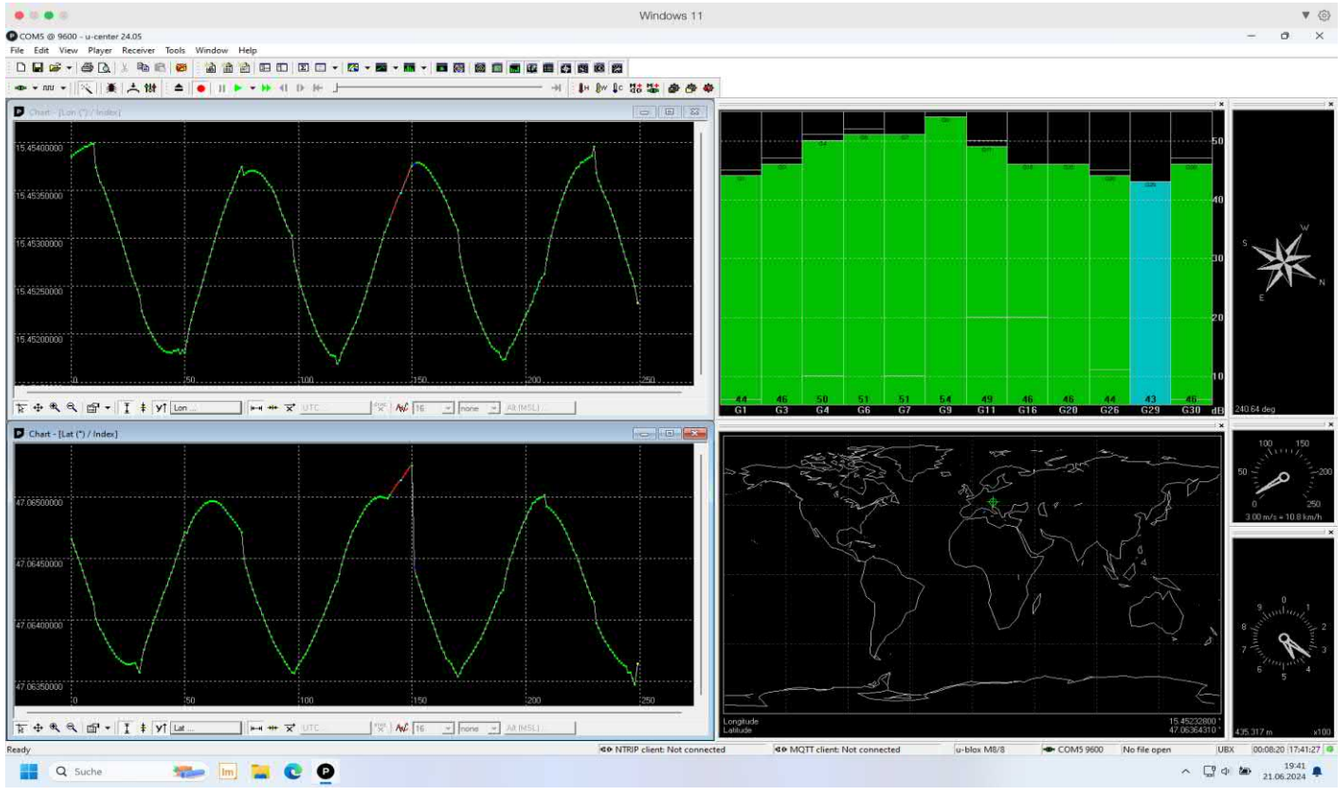


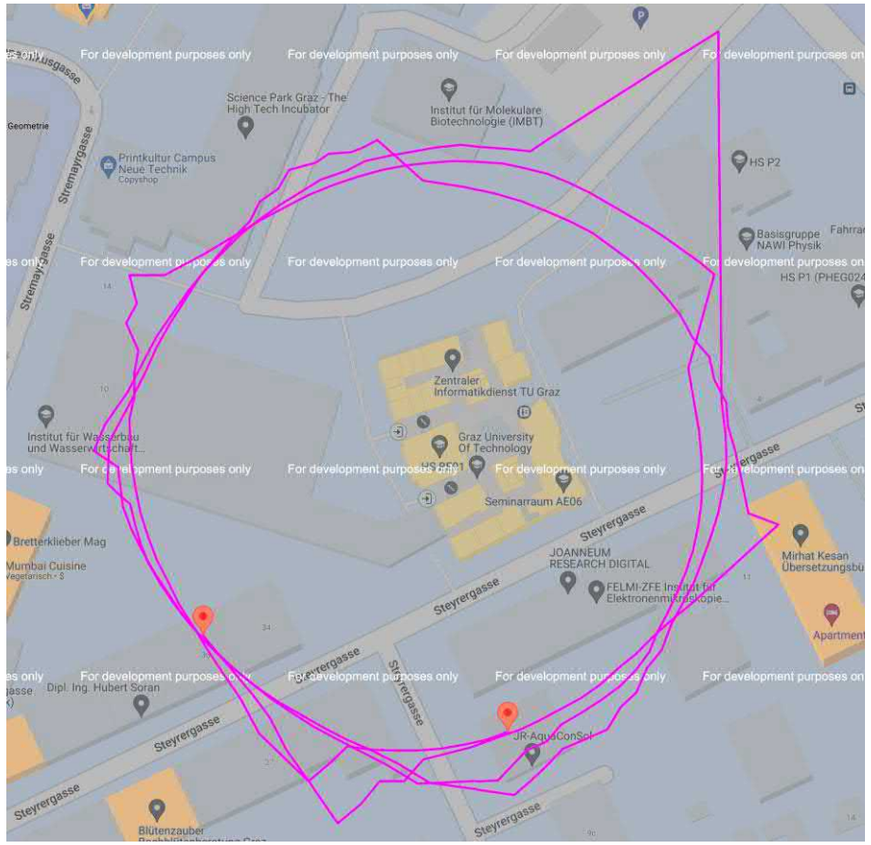


The possession and use of jammers and spoofers of any kind is illegal throughout the EU!

Research as part of a bachelor's thesis

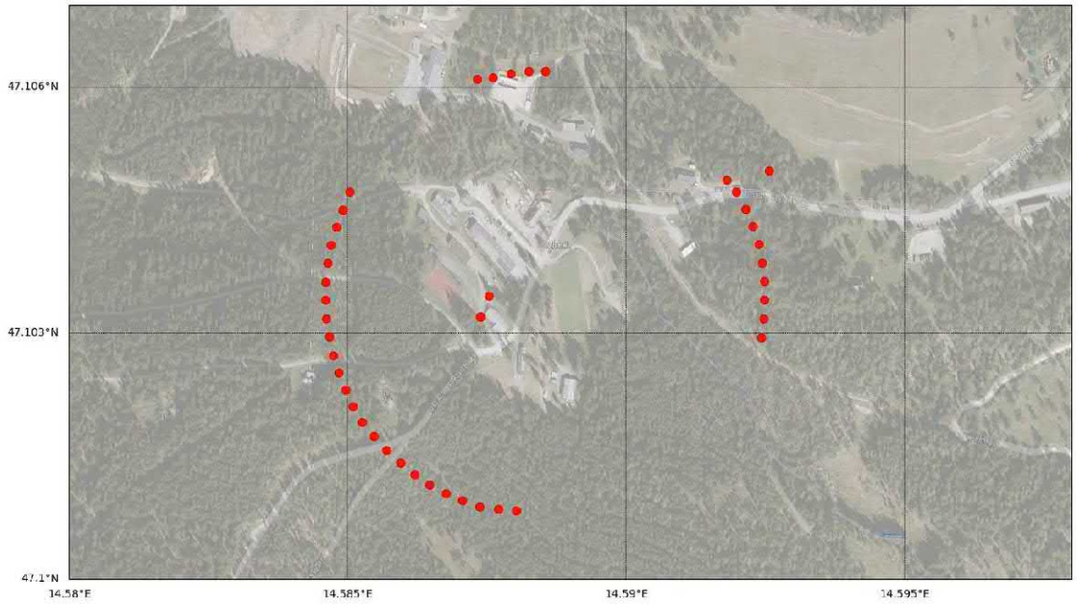
- Aichner Tobias (2024): Untersuchung von Spoofing-Vorfällen: Auf den Spuren eines GNSS-Mysteriums. Bachelor Thesis at TU Graz, Institute of Geodäsie, 2024.

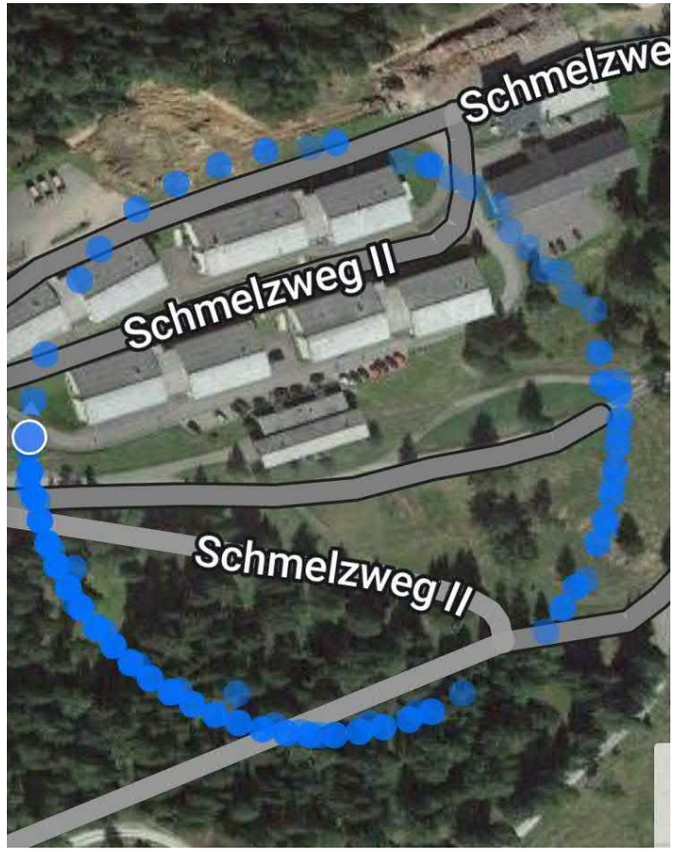


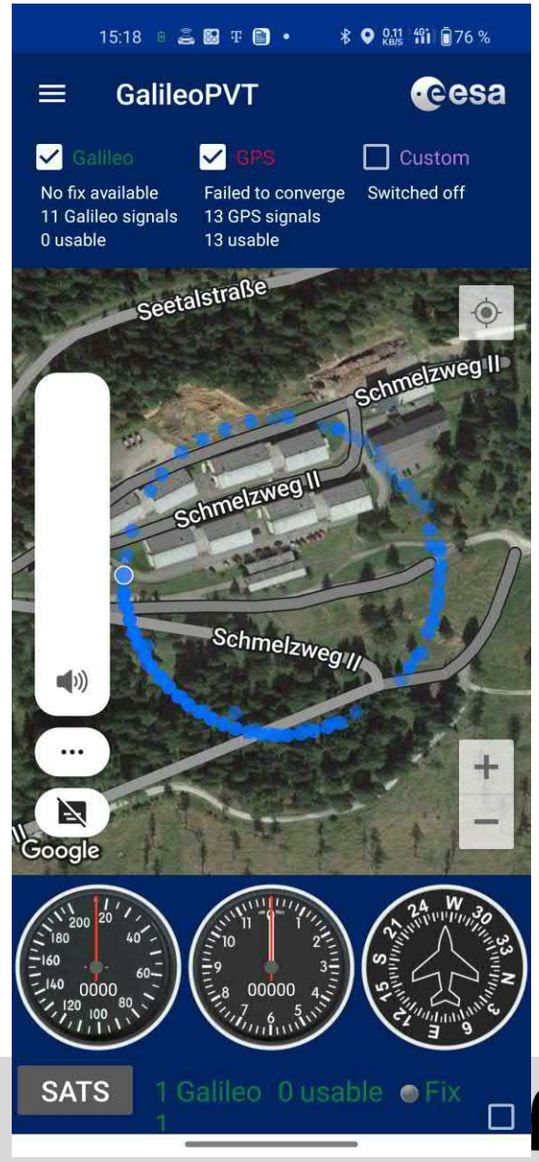


Demonstration of GNSS-Circle-Spoofing in Austria

- Circle-Spoofing successful
  - Test setup works
  - Radius 150 m
    → no continuous tracking







What can be done about it?

- Very simple spoofing → easily detectable

- Successful detection is a pre-requisite for mitigation
  - Monitoring on signal and/or range level
  - Use of other sensors in combination or as backup

- Countermeasures
  - Receiver autonomous integrity monitoring (RAIM)
  - Consistency with other sensors (e.g. IMU)
  - Cryptographic techniques (e.g. Galileo OSNMA, Galileo PRS, Galileo SAS)
  - Multi antenna arrays (e.g. adaptive nulling, beamforming)
  - Vestigial signal defence (e.g. correlation peak monitoring)

Summary

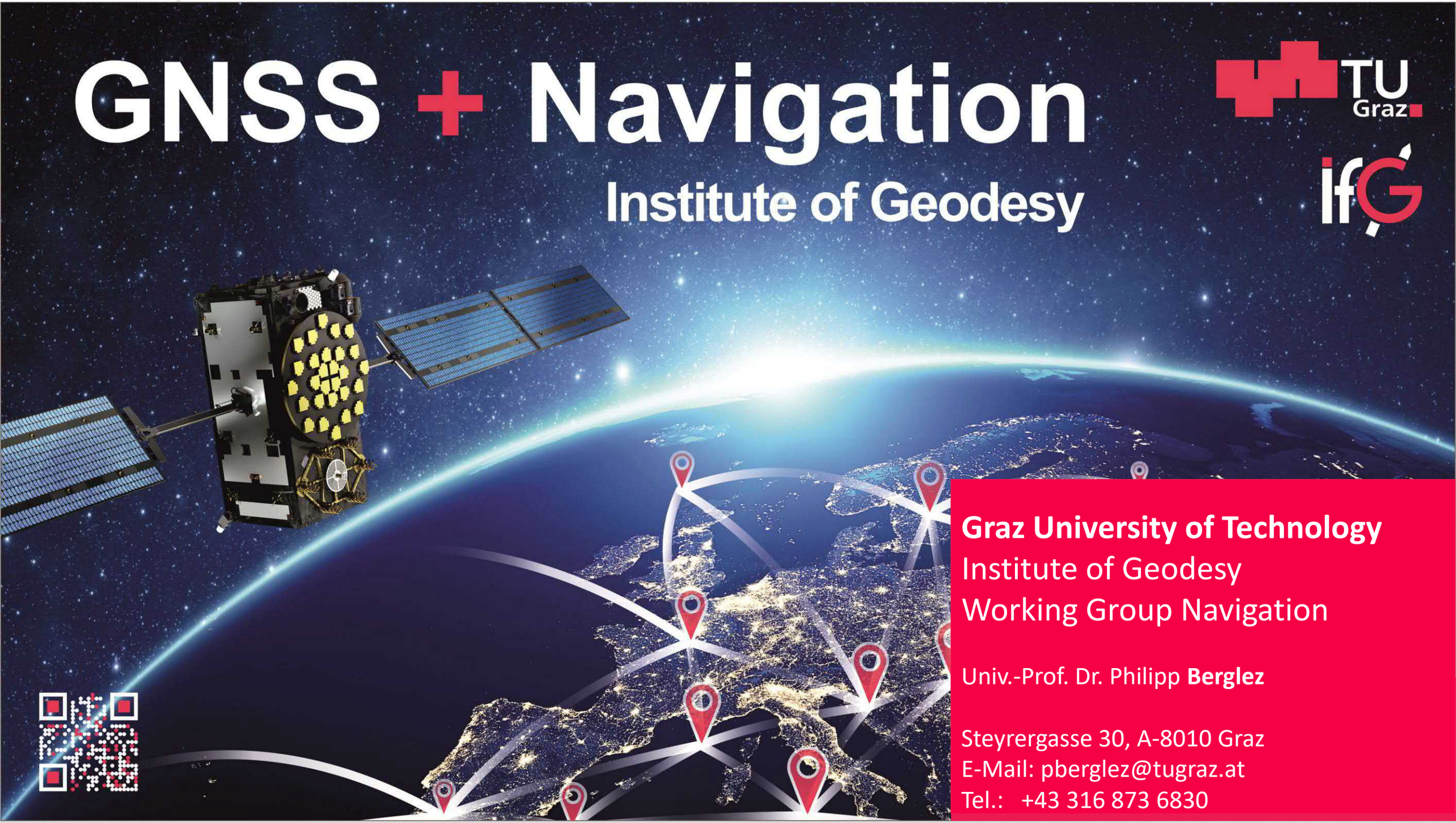
- Intentional interference with GNSS signals poses a major threat to users
  - Jamming
  - Spoofing
- Users expect accuracy, availability, reliability and robustness
- Detection, classification and localisation enable the use of countermeasures.
- Risk analysis in the field of GNSS is now more important than ever.

Ref.: http://wednesdaywilsondownunder.blogspot.com

Be aware, know the risk, monitor your GNSS and be prepared!

GNSS + Navigation

Institute of Geodesy



Graz University of Technology
Institute of Geodesy
Working Group Navigation

Univ.-Prof. Dr. Philipp **Berglez**

Steyrergasse 30, A-8010 Graz
E-Mail: pberglez@tugraz.at
Tel.: +43 316 873 6830