Norwegian Communications Authority

Jammertest in Norway in 2022 and plans for 2023

Safety and Security Issues in Positioning, Navigation and Timing,

NNF seminar, 14.06.23

Background

- The RFI situation
  - The RF environment that GNSS signals have to exist in, have become less safe over the last years. This is a trend Norwegian authorities expect to continue
  - GNSS signals are weak and can therefore easily be jammed, and the civil signals are open so they can “easily” be spoofed

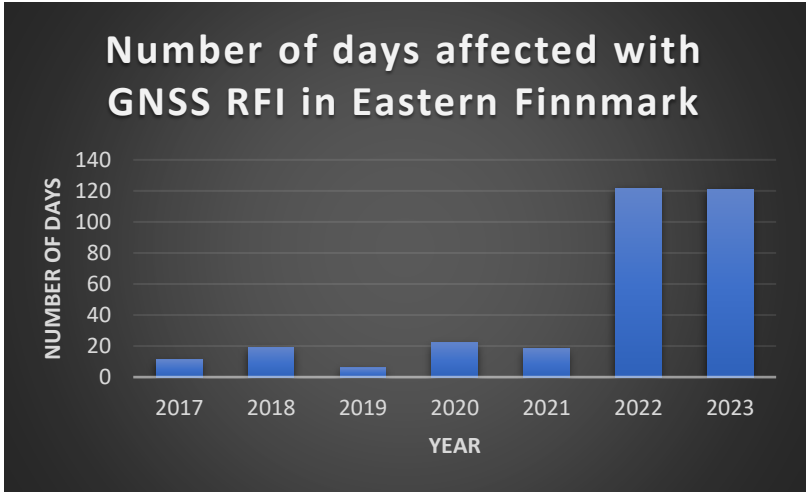
Samordningsforum for GNSS

→ Testfest 2021

→ Jammertest 2022

→ Jammertest 2023

→ 2024++



What do we want to achieve?

The purpose behind doing large scale jamming and spoofing in real world environments can be summed up as:

- Increase public awareness about the dangers of jammer use
- Increase competency in relevant authorities
- Motivate, facilitate and aid industry and academia to make and produce more robust equipment, that also can properly detect GNSS RFI

We want to bring together experts and problem owners in the field to look at GNSS vulnerability in order to get even better and more robust solutions on the market.

We believe in doing this by working together and sharing with each other as much as everyone is comfortable with sharing.

Also, can we think new regarding regulation?

- The classic approach:

New technology → new problem → new regulation

  - ❑ Becomes increasingly difficult as technologies become complex and more and more authorities are involved

- The pilot approach:

Technology → potential new problem → new technology

  - ❑ Demands a lot of cooperation and trust

- Jammertest is a product of R&D combined with the wish and will to think new
- The vision:

  There is not supposed to be space in the market for actors who are not robust against GNSS RFI!

19th to 23rd of September, 2022, Andøya

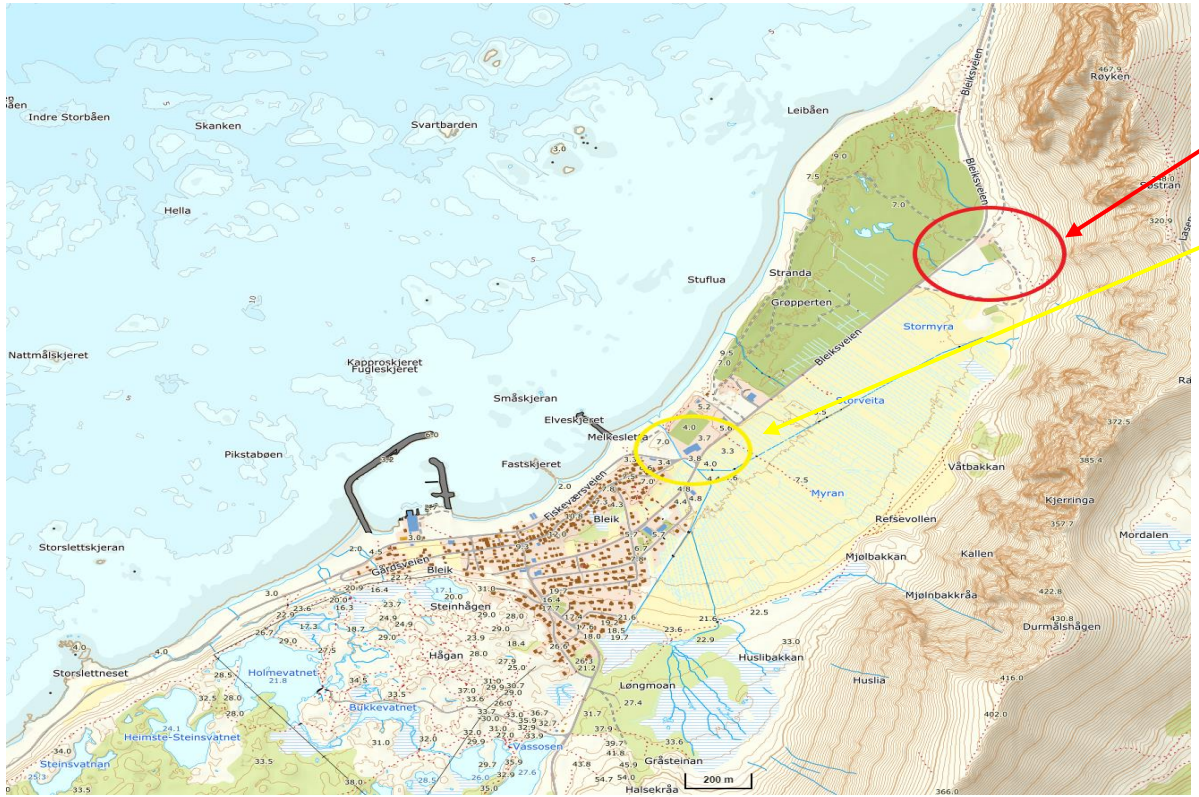
Jamming and spoofing of GNSS in real life environments

Jammertest 2022

Jammertest 2022 - locations

- Andøya, Nordland
- Tests were mainly performed around the village of Bleik

Jammertest 2022 - locations



- High effect jammer (max 20 W)
- Base camp
  - Storage
  - Power
  - Food, etc.
  - Low effect jammers
  - Spoofing

Jammertest 2022 – program and participants

Session	Main activity
Monday ***after lunch***	General static tests of high-effect jammer and of low-effect/personal jammers
Tuesday ***before lunch***	Jamming: Step-up tests and tests of different signal types and frequency bands
Tuesday ***after lunch***	Jamming: Continue with step-up tests and tests of different signal types and frequency bands – Tests with jamming over longer time periods.
Wednesday ***before lunch***	Jamming: Driving tests on roads with static high- and low-effect jammers
Wednesday ***after lunch***	Jamming: Driving tests on roads with dynamic jammers
Thursday ***before lunch***	Spoofing: Fundamental spoofing attacks
Thursday ***after lunch***	Spoofing: Trial of more advanced spoofing attacks
Friday ***before lunch***	New ideas tests Demonstrations tests

Industry	Service providers	Research institutions	Users	Authorities
Ublox Kongsberg Teledyne Radionor Q-Free GPSPatron AD Navigation Hexagon Spirent	Fugro GS Group	SINTEF NTNU FGI FFI Kartverket DTU Space	Telenor Statnett Luftambulansen Redningshelikopter-tjenesten Volvo Cars Andøya Space Sjøforsvaret Kystverket Luftforsvaret Norsk landbruksrådgivning NORA EWCC Norwegian Special Mission	Norsk Romsenter Nkom Styrelsen for Dataforsyning og Infrastruktur (dansk myndighet) Vegvesenet Justervesenet KDD

Jammertest 2022 – Example day (Tuesday)

Step up tests, from 2 nW to 20 W EIRP (100 dB dynamics)

- L1 CW
- L1 PRN
- L1, G1, L2, L5 CW
- L1, G1, L2, L5 PRN
- L1, L5, E5b CW
- L2, L5, G2, E5b CW
- L2, L5, G2, E5b PRN

Long time jamming

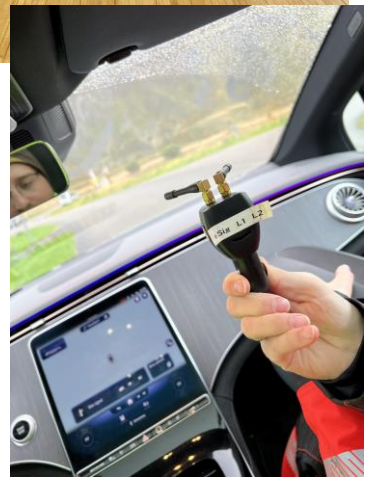
Pyramid

- E5b
- Eb5, L5
- E5b, L5, G2
- E5b, L5, G2, L2
- E5b, L5, G2, L2, B1l
- E5b, L5, G2, L2, B1l, G1
- E5b, L5, G2, L2, B1l, G1, L1
- E5b, L5, G2, L2, B1l, G1
- E5b, L5, G2, L2, B1l
- E5b, L5, G2, L2
- E5b, L5, G2
- E5b, L5
- E5b

Grunvatn

Jammertest 2022: Tuesday

UAS flying and motorcades



Jammertest 2022 – example of spoofing attacks

Advanced spoofing										
Initial conditions										
Signals	**Test #**	**Eph**	**Pos**	**Time**	**Initial jamming**	**Continous jamming**	**Scenario**	**Estimated start**	**Estimated duration**	**Comments**
GPS L1 C/A Galileo E1	Test 10	True	True	Synchronised	All bands/signals	All except L1/E1	Static position + motion	1400	20-30 min	
	Test 11	True	True	Synchronised	All bands/signals	None	Static position + motion	1430	20-30 min	
	Test 12	True	True	Synchronised	None	None	Static position + motion	1500	20-30 min	
	Test 13	True	True	Synchronised	All bands/signals	All except L1/E1	Static position + drift in time (frequency step)	1530	20-30 min	
	~~Test 14~~	~~True~~	~~True~~	~~Synchronised~~	~~All bands/signals~~	~~None~~	~~Static position + drift in time (frequency step)~~	~~1600~~	~~20-30 min~~	
	Test 15	True	True	Synchronised	None	None	Static position + drift in time (frequency step)	1630	20-30 min	
	Test 16	True	True	Synchronised	All bands/signals	All except L1/E1	Inject leap second	1700	15 min	
	Test 17	True	True	Synchronised	All bands/signals	All except L1/E1	Remove leap second	1715	15 min	

Jammertest 2022 - some interesting experiences

- *The satellite navigation systems in board a vehicle behave very differently from for example precise time servers. As both the margin of error and the consequences for the different systems differ, the GNSS implementation in the tech stack and the system response make it hard to say anything on a general basis. However, let me present some interesting cases*
  - Multi-GNSS systems are often dependent on a reference constellation, so that attacks against this constellation can degrade the PVT-solution, even with other healthy constellations, and in some cases completely deny service
  - Jamming can cause spoofing like symptoms, illustrating that some receivers have very high fault tolerance (fault tolerance vs satellite fix)
  - Different phases in the attack can produce different results, and the results can linger even long after the RF environment was healthy again (and in some cases never to recover). These transitions phases can be very unsafe places for GNSS receivers, even if they have well designed protection measures (usually made for jamming/no jamming cases)
    - Initiating RFI
    - Continuous RFI
    - Discontinuing RFI
  - Non-coherent spoofing works in when systems have no or bad security barriers, and/or in combination with jamming, ++
  - Coherent spoofing attacks work very well, and often did not need any jamming to succeed. Also, some multi-GNSS systems dependent on a reference constellation was completely spoofed by only spoofing that constellation, even though other constellations (and frequencies) were healthy
  - Even what looked like successful security measures could be spoofed if the spoofer was active for long enough (the new spoofed RF environment became the «real» environment, and when the healthy RF environment came back, this was seen as a new attack)

Jammertest 2023

18th to 22nd of September, 2023, Andøya

Jamming, spoofing and meaconing of GNSS in real life environments

Jammertest 2023 - locations

- Three locations, where one can work in parallel

1. Main high effect jammer and spoofing and meaconing attacks
2. Low effect jammers, «sandbox»
3. Jammers in cars, with long stretches of different types of roads. Motorcade type of tests

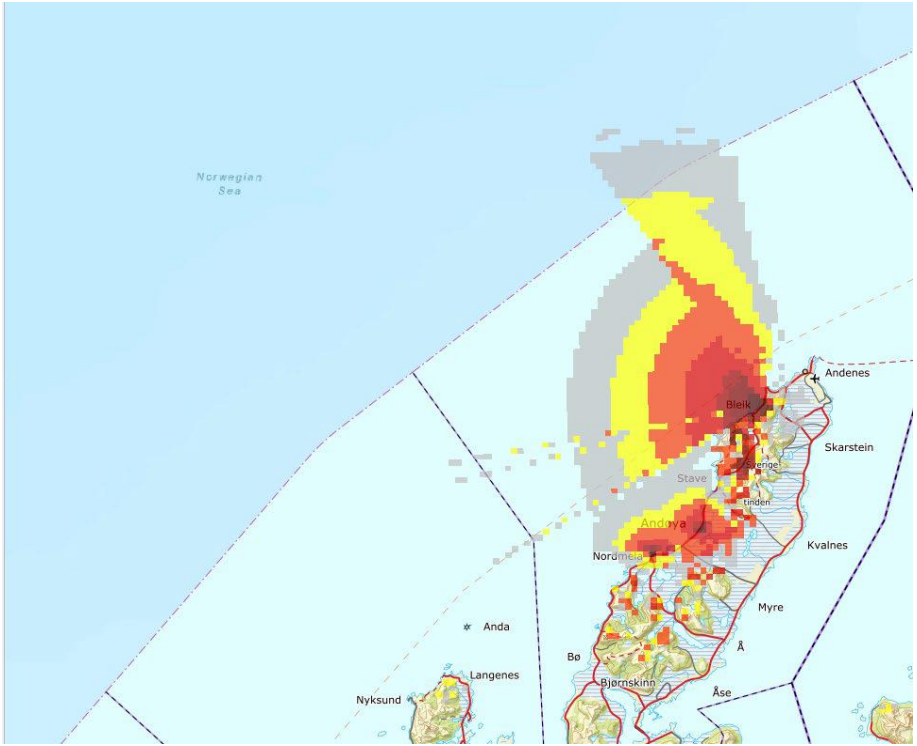
- Participants can roam freely between these three locations

Jammertest 2023 – affected areas

- Signal propagation

  Altitude: 5 feet

  Case 1: High effect jammer at the cemetery

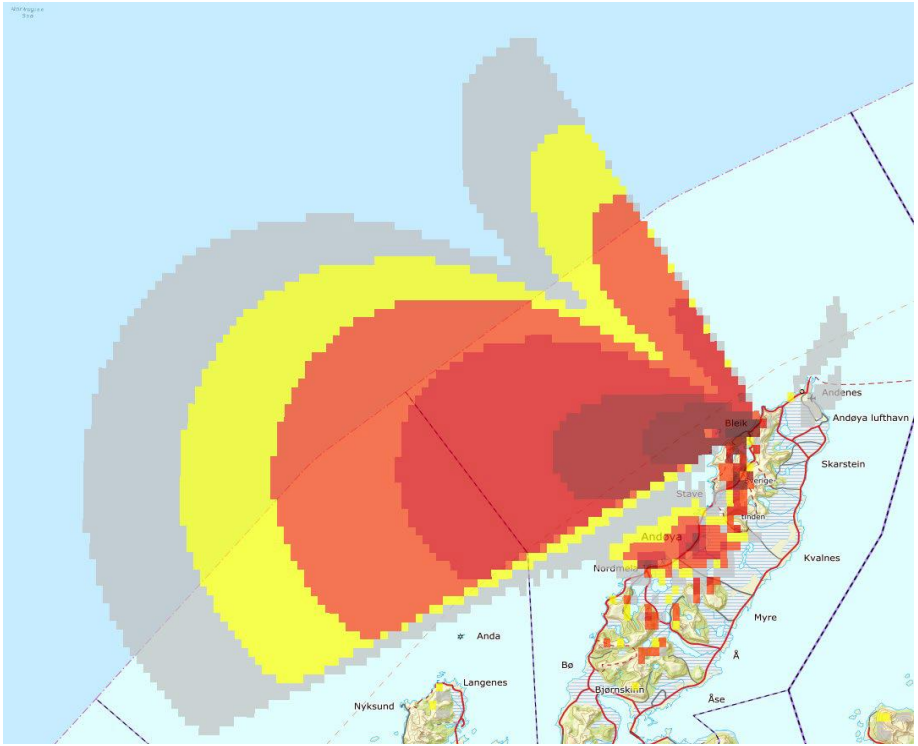


Jammertest 2023 – affected areas

- Signal propagation

  Altitude: 5 feet

  Case 2: High effect jammer at Alomar (mountain side)

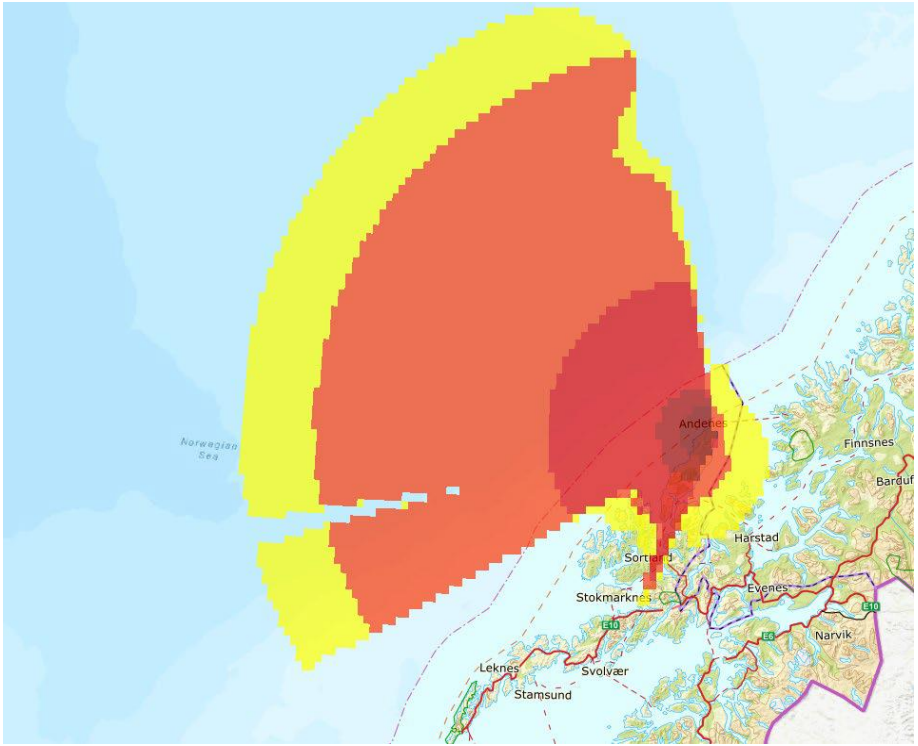


Jammertest 2023 – affected areas

- Signal propagation

  Altitude: 10 000 feet

  Case 1: High effect jammer at the cemetery

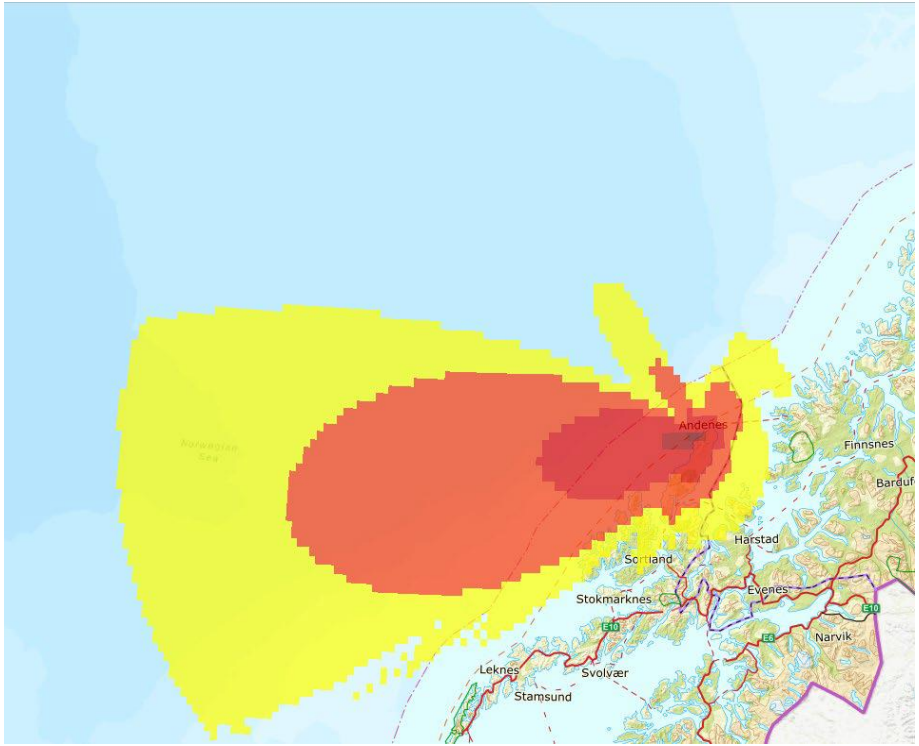


Jammertest 2023 – affected areas

- Signal propagation

  Altitude: 10 000 feet

  Case 2: High effect jammer at Alomar (mountain side)



Jammertest 2023 - Program

Day	Location 1 (Bleik)	Location 2 (Grunnvatn)	Location 3 (Stave-Nordmela)
Monday (18.09.23)	High effect stationary jamming (from lunch)	Book time slots on hourly basis Low effect jammers	Low effect stationary jamming (from lunch)
Tuesday (19.09.23)	High effect stationary jamming Multi-jammer scenarios	Book time slots on hourly basis Low effect jammers	Motorcade (with low effect jammers) Based on industry input
Wednesday (20.09.23)	Stationary meaconing Stationary spoofing Mainly position, navigation	Book time slots on hourly basis Low effect jammers	Motorcade (with low effect jammers) Based on industry input
Thursday (21.09.23)	Stationary meaconing Stationary spoofing Mainly timing	Book time slots on hourly basis Low effect jammers/Multi-jammer scenarios	Mobile meaconing (SDR) Mobile spoofing (SDR) Mainly position, navigation
Friday (21.09.23)	Rest, demonstrations (to lunch)	Rest (to lunch)	Rest (to lunch)

Jammertest 2023 - Participants

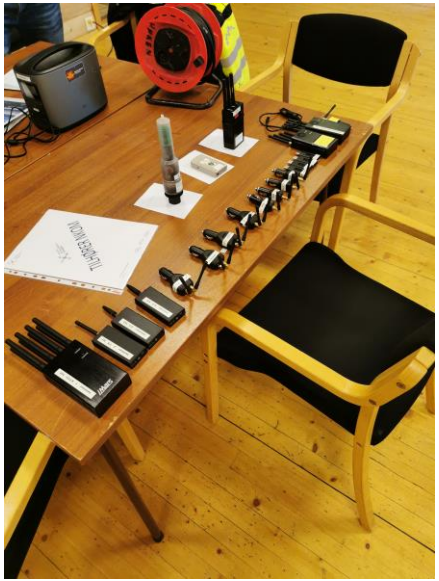
- Norway, Poland, France, Italy, Finland, Czech Republic, Israel, Japan, Sweden, Germany, Canada, UK, the Netherlands, Belgium, US

Thank you for the attention ☺

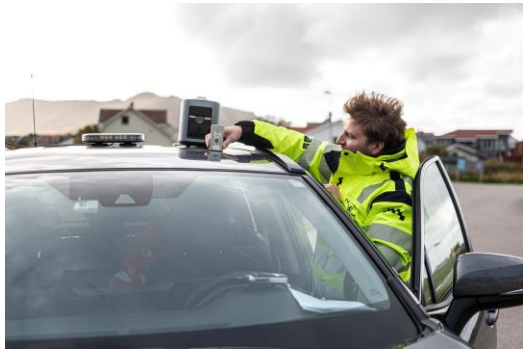
Extra: Jammertest 2022 Monday

Testopplegg:

- Tests of all low effect jammers at Bleik
- Test of high effect jammer (Cemetery)
  - L1 CW
  - L1 PRN
  - L1, G1 CW
  - L1, G1 PRN
  - L1, G1, L2 CW
  - L1, G1, L2 PRN
  - L1, G1, L2, L5 CW
  - L1, G1, L2, L5 PRN
- Sandbox tests at Grunnvatn



Extra: Jammertest 2022 Monday



Extra: Jammertest 2022 Wednesday

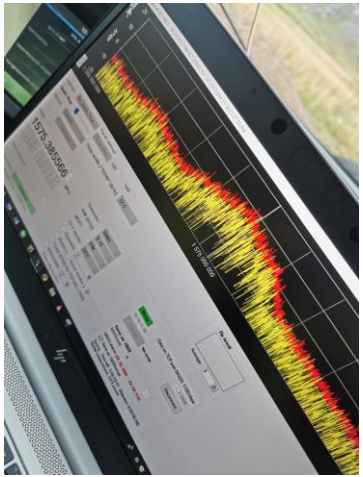
UAS flying and motorcades

Tests:

Long time jamming

Motorcades with jammers in and around the vehicles

Sandbox at Grunvatn



Extra: Jammertest 2022 Thursday

Spoofing (of GPS L1 C/A & Galileo E1)

- Different combinations of jamming and spoofing transmissions

Tests:

- Noen-coherent attacks
- Coherent attacks

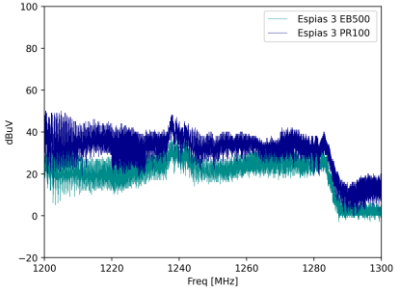
Extra: Some details (Jammertest 2022)

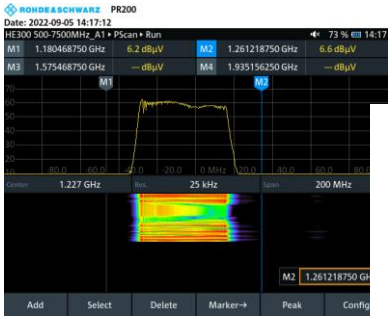
- High effect jammer used a P code modulation
  - Directional antenna with 20 W EIRP

- The spoofer was a passive isottropic antenna with 62 dBm to -29 dBm EIRP

High effect jammer at the Cemetery		
Jamming signal	Center frequency (MHz)	BPSK modulation rate (MHz)
L1	1575,42	10,23
L2	1227,6	10,23
L5	1176,45	10,23
G1	1602	5,11
G2	1246	5,11
E5b	1207,14	10,23
B1I	1561,1	2

Extra: Some details (Jammertest 2022)



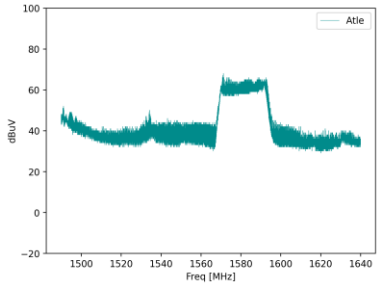


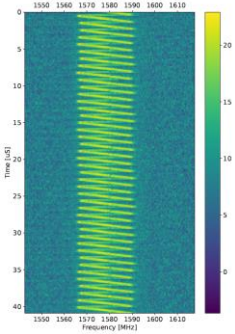
Jammer 12 - «Skipper»

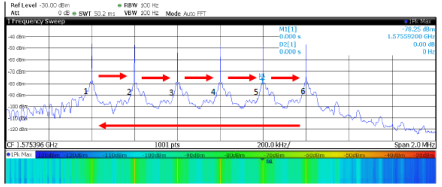
Frequency-hopping jammer.

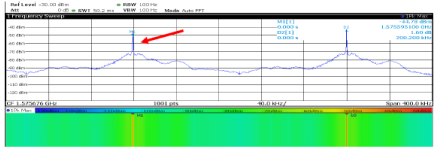
Signal form:

- Pulsed CW, signal duration of ~9ms~
- Every 50 ms, the CW-frequency is increased with ~200kHz
- After five increments, the CW-frequency is reduced with ~1000kHz (back to start)
  - Frequency #1 – 1574.62 MHz
  - Frequency #2 – 1574.82 MHz
  - Frequency #3 – 1575.02 MHz
  - Frequency #4 – 1574.62 MHz
  - Frequency #5 – 1574.62 MHz
  - Frequency #6 – 1574.62 MHz









Extra: Some details (Jammertest 2022)

- Example:

Jammer 12 «Skipper»

Jammer 12 - «Skipper»

Frequency-hopping jammer.

Signal form:

- Pulsed CW, signal duration of ~9ms~
- Every 50 ms, the CW-frequency is increased with ~200kHz
- After five increments, the CW-frequency is reduced with ~1000kHz (back to start)
  - Frequency #1 – 1574.62 MHz
  - Frequency #2 – 1574.82 MHz
  - Frequency #3 – 1575.02 MHz
  - Frequency #4 – 1574.62 MHz
  - Frequency #5 – 1574.62 MHz
  - Frequency #6 – 1574.62 MHz