engineering proceedings

MDPI

Proceeding Paper

Jammertest: An Open GNSS Interference Test Arena to Accelerate the Development of Resilient GNSS Applications †

Nicolai Gerrard [1,*], Tor Atle Solend [2], Anders Rødningsby [2], Øystein Karlsen [1], Tomas Levin [3], Harald Hauglin [4], Kristian Svartveit [5], Christian Berg Skjetne [3], Anders Martin Solberg [6], Thomas Rødningen [4] and Øystein Borlaug [2]

[1] Norwegian Communications Authority, Nygård 1, 4790 Lillesand, Norway; oyk@nkom.no
[2] Norwegian Defence Research Establishment, Instituttveien 20, 2007 Kjeller, Norway; tor-atle.solend@ffi.no (T.A.S.); anders.rodningsby@ffi.no (A.R.); oystein-dag.borlaug@ffi.no (Ø.B.)
[3] Norwegian Public Roads Administration, Postboks 1010 Nordre Ål, 2605 Lillehammer, Norway; tomas.levin@vegvesen.no (T.L.); christian.berg.skjetne@vegvesen.no (C.B.S.)
[4] Norwegian Metrology Service, Fetveien 99, 2007 Kjeller, Norway; hha@justervesenet.no (H.H.); thr@justervesenet.no (T.R.)
[5] Norwegian Space Agency, Drammensveien 165, 0277 Oslo, Norway; kristian.svartveit@spaceagency.no
[6] Norwegian Mapping Authority, Kartverksveien 21, 3511 Hønefoss, Norway; anders.martin.solberg@kartverket.no
* Correspondence: nicolai.gerrard@nkom.no
† Presented at the European Navigation Conference 2025 (ENC 2025), Wrocław, Poland, 21–23 May 2025.

Abstract

Jammertest, held annually in Andøya, Northern Norway, is the world's largest open test for evaluating the resilience of Global Navigation Satellite System (GNSS) technologies against jamming, meaconing, and spoofing threats. Set in a remote Arctic location ideal for high-power interference testing with minimal societal impact, the event brings together a wide range of participants, from academia and industry to government agencies, to conduct real-world GNSS interference testing from a comprehensive and up-to-date Test Catalogue. Organised by a coalition of Norwegian authorities, Jammertest offers a unique environment and an inclusive approach to foster advancements in GNSS resilience without relying on strict regulation. This paper describes the background, approach, and technical setup, such as the transmissions, for the test week.

Keywords: GNSS RFI; resilience testing; jamming; spoofing; meaconing; Jammertest; Norway

1. Introduction

Since the conception of GPS, and especially after the discontinuation of the Selective Availability in 2000, Position, Navigation, and Timing (PNT) information from satellites has become enormously widespread around the globe. Today referred to with the common designation Global Navigation Satellite Systems (GNSS), the services, industries, and critical infrastructure that this PNT supports is overwhelming: from providing Low-Earth-Orbit (LEO) satellites with their positioning to optimising agriculture. GNSS has become an integral part of most aspects of modern society, and its use is estimated to continue to grow [1].

However, as a radio-frequency-based technology, GNSS is susceptible to the same threats as all other radio technologies: namely, radio frequency interference (RFI). This has been known for as long as the satellite systems have existed; however, it gained more widespread attention with a 2001 U. S. Department of Transportation report [2], which put the focus on the vulnerabilities in GNSS to such RFI. Since then, the quality, ease of use,

Check for updates

Academic Editor: Tomasz Hadaś

Published: 24 February 2026

Copyright: © 2026 by the authors. Licensee MDPI, Basel, Switzerland. This article is an open access article distributed under the terms and conditions of the Creative Commons Attribution (CC BY) license.

and overall low cost of the service has pushed GNSS to become the primary PNT provider, and in many instances the only source for users worldwide.

This trend, particularly when it affects critical infrastructure and services essential to national security and daily life [3], has created significant and widespread dependencies [4]. Since PNT information is often an "invisible" resource, system-in-system vulnerabilities have occurred without the accompanying awareness of the RFI liabilities inherent in GNSS.

Lately, an increasing number of GNSS-dependent companies and organisations desire to test their systems and equipment for these vulnerabilities. This is based on a growing understanding of the dangers of RFI and the increasing amount of GNSS RFI in the world in general [5–7]. GNSS RFI has evolved from being an occasional nuisance to now being the new normal, e.g., in aviation [8], along highways [9], and even on construction sites [10]. The need for testing was expressed in discussions in a forum of Norwegian authorities through the years 2018–2020. As a result, the Norwegian Public Roads Administration (NPRA), along with a few other authority partners and industry participants, initiated a pilot test bed in 2021. The experience, feedback, and results were so promising that the next year, a consortium consisting of NPRA, the Norwegian Defence Research Establishment (FFI), the Norwegian Communication Authority (Nkom), and the Metrology Service (JV) launched a full week of operative GNSS interference testing in and around the village of Bleik in Andøya, Northern Norway. Later, two more Norwegian governmental agencies joined the consortium: the Mapping Authority (NMA) and the Space Agency (NoSA). In 2025, Avinor also joined as a partner.

This paper gives an overview of the testing, motivations, locations, and transmissions performed in Andøya during what has become an annual test week known as Jammertest. Previous works authored by some of the Jammertest organisers [11–13] have given an outline of the testing, but this work intends to give a more holistic synopsis of the why, how, and where, as well as a more detailed technical description of the transmissions and their rationales.

2. The Norwegian Approach

The concept of Jammertest is founded on a few key values, many of which are integral to Norwegian public life: facilitation, transparency and openness, cooperation, resilience building over time, and an alternative to strict regulation.

2.1. Facilitation

Because of the low power of the received GNSS signals, regulation and enforcement of the use of GNSS signals for anything else than SPACE-TO-EARTH radionavigation is extremely strict. Only in very special circumstances are terrestrial broadcasts allowed in most countries, then mainly for military exercises (e.g., [14]). The lack of options for such transmissions, together with the growing need for testing, is the general motivation behind Jammertest: to facilitate industry, academia, and authorities to test their equipment and perform experiments in live-sky GNSS interference environments out in the open. Sometimes the lab becomes too clean, too synthetic, or too physically restrictive (e.g., flying helicopters, driving cars), or there is a lack of technical know-how on how to produce what RFI signals. By providing all of this in the field and in one place, Jammertest aims to facilitate resilience and innovation across a broad range of sectors. Organising an annual event also concentrates tests into a single week to reduce the disruption to society.

2.2. Transparency and Openness

Transparency is central to Jammertest, reflecting broader Norwegian public values. All test-related information—technical and practical—is first shared with participants, then

archived on the official website [15]. The development of the Transmission Plan (TP) and Test Catalogue (TC) is public, with documents available in both JSON and PDF formats on the Jammertest GitHub [16]. The planning process is open to contributions, and after each Jammertest, technical details like the TP, TC, and logs are published [17].

Participants are free to use their own recorded data without restrictions. While sharing is encouraged to support the broader community, only acknowledgements in publications are requested. A library of public results is also maintained on the official site [18]. This openness ensures equal access to information, fosters collaboration, and supports continuous improvement.

2.3. Cooperation

In Norway, as in many countries, governance is sector-based. This poses challenges for addressing RFI, which affects multiple sectors and often leads to fragmented responsibility. Raising cross-sectorial awareness is therefore crucial. Jammertest has successfully performed this in Norway by elevating RFI on the agenda of key organisations and authorities. This was achieved through an organic development of roles and responsibilities, aligned with each organiser's strengths and expertise.

However, cooperation also extends to the participants. Participant involvement is an important part of Jammertest; partakers can request new and/or modified tests and put forward scenario ideas. The concept for test development is based on brainstorming among the organisers and from participant input. Testing far north of the arctic circle in a remote area also means that participants must cooperate to help each other. This, coupled with the diverse participation and their combined competencies and experiences, create a unique arena for not only testing but learning as well.

2.4. Resilience Building over Time

Discovering weaknesses or vulnerabilities in equipment, systems, and algorithms is extremely useful, but much less so if the patches and upgrades performed to improve upon them are not validated. Jammertest is thus an annual event where improvements can be tested towards the same RFI, and their value confirmed or rejected. In this manner the participant can evaluate implemented improvements from several visits to Jammertest and perform active debugging to more easily figure out which patches to implement next. This demonstrates the iterative value of testing and how the organisers believe Jammertest will contribute to increased GNSS RFI resilience: steps of improvement in many sectors and organisations repeated over time, coupled with as much sharing of results and ideas as possible. This has special importance since GNSS as systems-in-systems obscure many equipment liabilities and thus create uncertainties that must be explored.

2.5. An Alternative to Strict Regulation

From our perspective as organisers, we see Jammertest as an approach that offers an alternative to strict regulation by the government. The overall goal is to show that there should be no place in the market for devices and services that are not resilient to GNSS RFI. It should be a main selling point that your product has survived Jammertest. With strict regulation it is challenging to have the legislation keep up with the speed of innovation. Thus, Jammertest is intended to serve as an option to introduce resilient equipment into the market before strict regulation enters into effect.

2.6. What Is a Successful Event?

A simple indication of the usefulness of Jammertest is the ratio of the cost of organising the event to the time and cost incurred by the participants. A back-of-the-envelope calculation based on manhour use indicates that the benefit is somewhere between 40:1

and 60:1. This means that for every EUR 1 we spend, we receive back EUR 40 to EUR 60 in costs that the participants absorb.

A more technical indicator of success is whether the transmissions can defeat the systems that are tested. Since we do not collect information about the participants' vulnerabilities, we rely on them to publish findings, compiling relevant scientific and popular publications as evidence of impact.

As the event matures, increased system robustness is expected, driven by participant feedback and repeated testing. This is also expected of repeat visitors. Continued success depends on evolving test scenarios to reflect real-world threats—making creativity from both organisers and participants essential.

All in all, we call this process of building resilience through the facilitation of a transparent and open iterative testing based on cooperation and sharing, all to avoid very difficult regulation, *The Norwegian Approach*.

3. The Jammertest Event—The Practical Approach

3.1. The Location

Jammertest is held in the north of Norway on an island called Andøya. Andøya delivers on key aspects that makes the location close to perfect for field live-sky RFI testing. The mountains to the east of the small village of Bleik act as shields for the Norwegian mainland from the transmitted signals. To the west, the nearest neighbour across the Norwegian Sea is Jan Mayen, about 1000 km away. Andøya is a tourist destination in summer and has an airport. This means plenty of accommodation is available in September (the month of the test) for Jammertest. Additionally, the local inhabitants are used to military and restrictive activities, e.g., rocket launches. These aspects allow for testing that produces as little disturbance to civil society as possible.

Figure 1 gives an overview of the four locations used for testing during Jammertest. Their functions are:

1. The main test area, where the high-power jamming, meaconing, stationary advanced spoofing, and other types of RFI is performed.
2. The area for low-power jammer devices (e.g., Personal Privacy Devices (PPDs)), arranged in circular configurations and on drones, in addition to stationary and mobile spoofing and multi-direction transmissions.
3. The area for motorcades, where vehicles can test with low-power jammers placed inside the vehicles, inside or outside the motorcade, and perform mobile spoofing inside or outside the motorcade.
4. The local airport, where jamming is performed on aeroplanes, fixed-wing drones, and helicopters conducting instrument approach procedures on an active airstrip.

3.2. Execution of the Event

The nature of Jammertest warrants an explanation of the practical aspects.

3.2.1. Key Numbers

Table 1 summarises some key figures to illustrate the size and growth of Jammertest. For reference, the number of applicants for 2025 is 365.

https://doi.org/10.3390/engproc2026126020

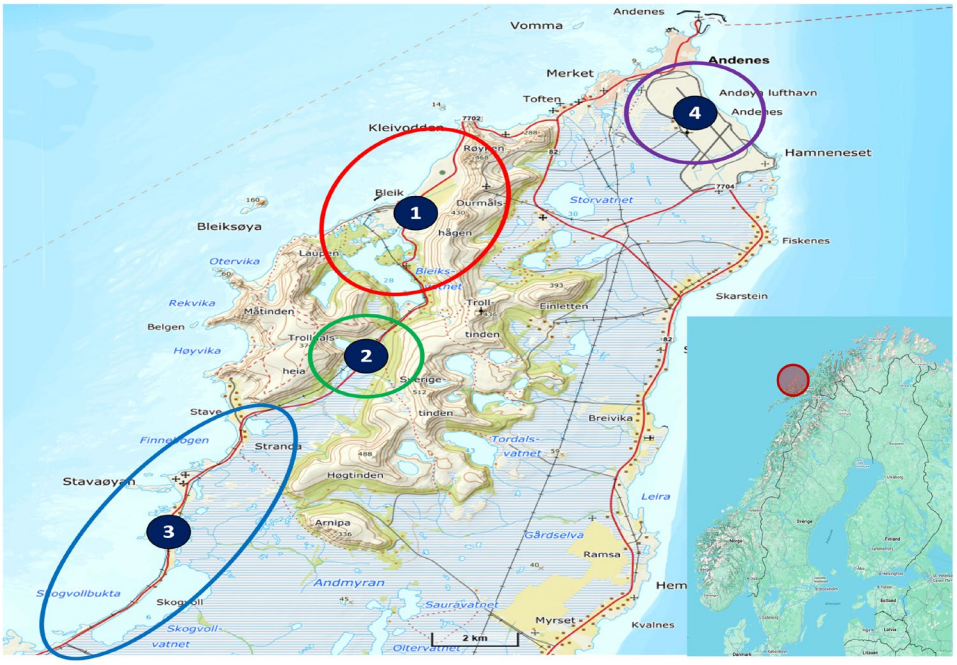


Figure 1. A map of Andøya indicating the four different test locations: (1) main test area, (2) jamming devices, (3) motorcade, and (4) airport. Insert: A map contextualising the location of Andøya.

Table 1. A count of the number of persons, countries and organisations that applied for participation and participated at Jammertest in 2023 and 2024.

Key Areas	# in 2024	# in 2023
Applications	267	182
Participants	230	160
Organisers	52	31
Nationalities	29	19
Organisations	97	64

3.2.2. Logistics

The remote location of the event presents logistical challenges, especially in transporting equipment. Some participants drive up to 3000 km, while others ship their gear—much of which is expensive or export-regulated. Andøya Space, the Norwegian military, and the local community assist with shipping, reception, and storage.

3.2.3. Health and Safety

With over 300 participants, safety is a top priority. Trained first aid personnel from Norwegian People's Aid are on site 24/7 and staff from the NPRA ensure road safety. Mandatory daily briefings and debriefings cover safety rules and regulation as well as technical plans, and high-visibility clothing is always required outdoors.

3.2.4. Communication

The ability to communicate efficiently is critical for both a successful execution of the event and for safety. The test leaders need to be able to communicate with all participants and the other organisers, and the participants also need the opportunity to communicate with the organisers. The official communication channels are as follows:

- Webpage/newsletter—This is the main communication channel used before the event.
- Chat—Both participants and organisers have access to a chat during the event. This allows for manageable dual communication between organisers and participants.

- FM radio channel—The event operates a FM radio channel to broadcast information. The radio station announces the start and stops of all tests and any important announcements during the event, as well as providing music and entertainment.
- MQTT—Started, stopped, and currently running tests are published on an MQTT feed (the same information as on FM RDS (radio text) and in the chat).

3.2.5. Division of Responsibilities

Since Jammertest is an event that is co-hosted by several governmental bodies, the division of responsibilities is critical for a successful execution. The following is a rough division of responsibilities:

- NPRA—Event lead, health and safety, and most practical and organisational issues during the event.
- Nkom—Transmissions, technical lead, and spectrum monitoring.
- FFI—Transmission and practical execution of the tests.
- JV—Transmission and practical execution of the tests. Distribution of reference time.
- NMA—Supplier of GNSS location reference data.
- NoSA—Financial and administrative support.

All organisers contribute with technical know-how and in the practical and technical planning. In addition, we have contracted Testnor [19] to help with logistics and practical issues before and during the event.

4. The Jammertest Event—The Technical Approach

Jammertest creates GNSS RFI environments with the use of jamming, spoofing, meaconing, and simulations of unintentional RFI. The following sections describe the equipment used to generate them, introduce the transmissions themselves, and give an overview of the test groups, starting with a description of the documentation.

4.1. Test Catalogue vs. Transmission Plan

The Test Catalogue (TC) and Transmission Plan (TP) are inspired by the Test and Measurement industry. For Jammertest, we needed a similar system that would allow us to progress with all sorts of GNSS RFI testing in a systematic and coherent manner. Thus, all the test concepts, other documentation, and specification needs were gathered in the TC. The schedule for where, when, and how the chosen tests from the TC will happen is in the TP. After the test week is finished, the participants receive an official log, including deviations from the TP, so that they can align their results in time with the transmissions. Figure 2 shows an example of a jammer description found in the TC.

Technical details on low-power jammer "S1.3"

The jammer S1.3 belongs to the 'Cigarette jammer' category of jammers. Such jammers are often installed in the cigarette lighter outlet in cars. They are intended to cover the car, and a given radius around the car.

S1.3 is an one-antenna, so-called "L1-only", jammer, disrupting only the upper L-band.



Technical characteristics of S1.3 (2024 measurements)

Centre frequency [MHz]	Bandwidth [MHz]	PSD [dBm/MHz]	TX total [dBm]	CF max [dBm]	Sweep rate [µs]	Modulation
1579.63	31.88	7.56	22.60	7.93	37.5	Sawtooth

Figure 2. An extraction from the Jammertest 2024 TC appendix, giving an example of characteristics of a specific jammer, to inform participants about the signal transmitted by this jammer.

4.2. The Signal Generators

4.2.1. Porcus Maior—The Big Jammer

The jammer employed at the main test area generates high-power jamming signals. It transmits on up to eight channels simultaneously and utilises two four-channel SDRs for signal generation. The output signal is attenuated with a programmable step attenuator and, to provide sufficient range, the signals are amplified before being transmitted by high-gain helical antennas. The jammer setup is visualised in Figure 3.

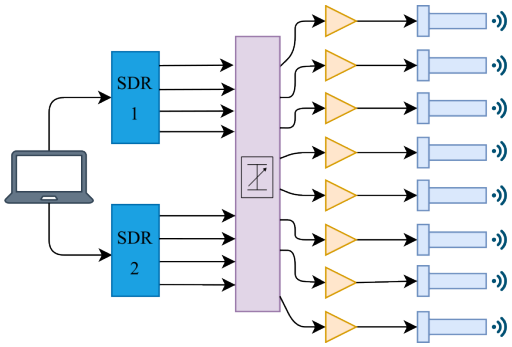


Figure 3. Jamming setup, from left to right: computer, NI Ettus USRP X410 (Ettus Research, Santa Clara, CA, USA), programmable step attenuator, RF amplifier, emitting antenna.

The jammer can generate many different signal modulations. During Jammertest, three different modulations are used: Continuous Wave (CW), Pseudo Random Noise (PRN), and Frequency Sweep (Sweep). CW is an unmodulated constant frequency signal with no bandwidth. PRN and Sweep are broadband signals with programmable bandwidth and other properties. In Table 2, the PRN and Sweep properties for the 2024 Jammertest campaign are summarised.

Table 2. Broadband jamming signal properties of Porcus Maior for the 2024 Jammertest.

PRN BPSK Chip Rate (MHz)	Sweep Rates (kHz)	Sweep Bandwidth (MHz)
3	1–100	6

In Table 3, the centre frequencies of the jamming signals are summarised. This applies to all signal types.

Table 3. The frequencies that Porcus Maior emits on.

Frequency Band Name	Frequency (MHz)	Frequency Band Name	Frequency (MHz)
L1	1575.42	G2	1246
L2	1227.6	E5b	1207.14
L5	1176.45	E6	1278.75
G1	1602	B1I	1561.098

4.2.2. Porcellum—The Meaconing System

A GNSS meaconing system re-transmits signals from a GNSS receiver. This principle requires that the receiving antenna is distanced properly away from the transmitting antenna to avoid creating a feedback loop between them. At Jammertest, the receiving antennas (1 and 2 in Figure 4) are positioned on the other side of the mountain ridge to the transmitter. Long fibreoptic cables connect the receiving antennas to the rest of the setup. The meaconing setup for the 2024 Jammertest is visualised in Figure 4.

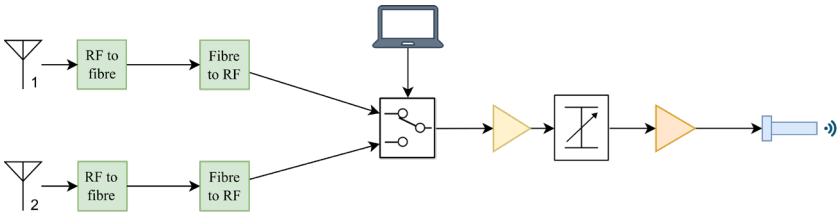


Figure 4. Meaconing setup, from left to right: GNSS receiver antenna, RF-to-fibre converters, programmable RF switch, RF amplifier, adjustable RF attenuator, RF amplifier, emitting antenna.

The RF signals from the receiving antennas consist of the L1 and L2 GNSS frequency bands. All other bands are filtered out. In the 2024 Jammertest setup, both signals were transmitted through the same amplifier and antenna. For the 2025 Jammertest, the signals will be split into two channels with respecting amplifiers and antennas.

4.2.3. Mobile SDR Spoofer

A mobile GPS spoofer has, up until the 2024 Jammertest, been used at the area for motorcades. The equipment consists of a laptop computer, an SDR, an RF amplifier, and a dipole transmitting antenna. The setup for the 2024 Jammertest was installed in a car and transmitted with an omnidirectional antenna from the car roof. The setup is somewhat rudimentary and is not synchronised with real GNSS time and thus differs in precision and accuracy compared to the spoofing conducted at the main test area.

4.2.4. "Low-Power" Jammers

There are plenty of jammers available to purchase online. They are illegal to use in most, if not all, countries, but that does not stop certain people from acquiring them. These types of jammers are also present at Jammertest. Nkom has procured a number of these devices, available for use in the first three test areas. They are divided into four groups:

- Handheld, battery-powered jammers
- Cigarette lighter socket/12 V outlet jammers
- USB-stick jammers
- Permanently installed/non-battery jammers

Most of the low-power jammers are within the first three groups, with a few exceptions. In Figure 5, some of the jammers are displayed, with labelling (white stickers and attached slips of paper) with reference to the TC for their RF characteristics.



Figure 5. The left picture shows some cigarette lighter socket jammers and the right picture shows handheld and permanently installed jammers, all available for use at Jammertest.

4.2.5. Stationary Spoofer

Spoofing signals at the main test area were generated using Ettus USRP X300 SDRs (Ettus Research, Santa Clara, CA, USA) controlled by Safran Skydel simulation software (version 24.6.0). Figure 6 illustrates the setup.

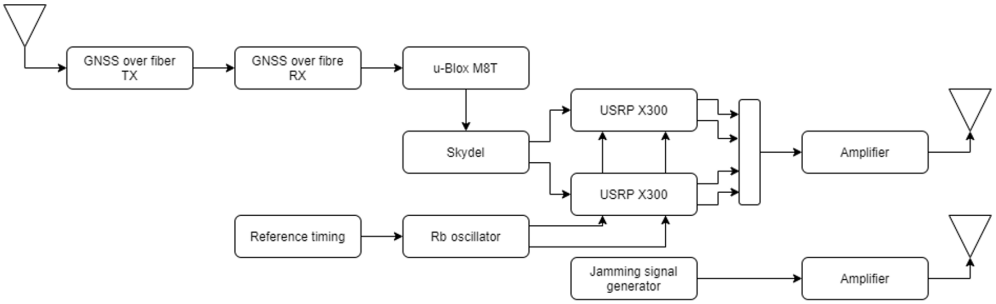


Figure 6. A schematic overview of the stationary spoofing setup employed at location 1 and the accompanying jammer system for transmission combinations.

These signals were transmitted via roof-mounted omnidirectional antennas at the Bleik community house, synchronised using a rubidium oscillator and a GNSS signal relayed over fibre from a remote, undisturbed location. The spoofing setup allowed for both coherent and incoherent spoofing scenarios, using real and synthetic ephemeris data sourced from, e.g., NASA [20]. The setup is designed to simulate realistic spoofing attacks with high timing precision, supported by a robust synchronisation infrastructure independent of local GNSS availability (coherent spoofing attacks align with real satellite signals, i.e., a receiver will "see" the new fake signals as just continuations of the recently received genuine signals, but with a very slight shift. This shift depends on how well the spoofing generator is synchronised to satellite time—the better synchronised, the smaller the shift. Incoherent spoofing attacks are the opposite, i.e., a receiver will "see" a new sky featuring new satellites in different combinations than the recently received genuine signals, thus making such attacks easier to detect). Further descriptions on the synchronisation setup can be found in [12].

4.3. The Transmissions

Table 4 gives an overview of the main transmission groups used at Jammertest, their rationales, and what type of tests they enable.

Table 4. An outline of the main groups of transmissions used at Jammertest (up until Jammertest 2025).

Transmission Group	Rationale
Stationary high-power jamming	Creates an RFI environment over a large area/space with tests built from "simple" (like CW on a single band) to complex (spectrum matching, like PRN, on many bands) signals. The large area allows for more dynamic testing with vehicles and airborne and maritime devices. Resilience testing is realised with different modulations, power, and band combinations, and the physically large RFI environment at location 1 allows for moving in and between natural (i.e., terrain, buildings, etc.) obstructions. Sensitivity can be tested with power ramps and jamming pyramids.
Stationary low-power jamming	Simulates real-world scenarios where one is affected by devices acquired by, e.g., private citizens, criminals, etc. Can be installed in many different topographical configurations to, for example, challenge CRPAs and detection mechanisms.
Mobile low-power jamming	Same as for stationary low-power jamming, just with the additional complexity of movement. Can be placed in cars, boats, drones, etc., to simulate, for example, meeting a car with a jammer, being radiated from above, etc.
Stationary spoofing	Creates environments with false (generated deception) signals from a stationary spoofer, to make the environments as stable as possible. Tests resilience through increasingly complex attack vectors; incoherent GPS-only high power to coherent multi-band and -constellation power ramps, with initial and continuous jamming. Affected areas are large enough to also perform dynamic tests.
Stationary meaconing	As a deception attack that just relays original signals, meaconing tests can potentially be harder to detect and can potentially evade defences based on encryption and authorisation. Affects a larger area, which allows for dynamic testing with vehicles and airborne and maritime devices. Can be combined with jamming to test band and technology preferences and fallbacks.
Mobile spoofing	Same as for stationary spoofing, but with the additional complexity of moving the transmitter.

5. Conclusions

Jammertest is a unique annual event bringing together participants from all over the world to test GNSS equipment under a live sky with intentional GNSS RFI. Its uniqueness arises from both the normal inaccessibility of such live-sky testing events and what the organisers have coined "*The Norwegian Approach*": a collaborative, transparent, and facilitative method for building resilience through open, real-world testing environments, with emphasis on cooperation across sectors and iterative improvements over time.

The event is the result of strong cooperative effort between the organising partners. This has led to a comprehensive and unique event that fulfils a demand coming from the whole value chain of GNSS—from space system owners, through receiver and chip manufacturers and system integrators, to end users.

Its novelty lies in constantly evolving test facilitation and the development of new test concepts based on results from previous Jammertests, the evolving global RFI environment, and new ideas and ingenuity from within the GNSS community. The test scenarios are a mix of known RFI and original transmission scenarios, and the ensemble has to be kept up-to-date and relevant to keep the main event useful and to foster potential offshoots in the form of specialised tests trails.

Author Contributions: Conceptualisation, N.G.; writing—original draft preparation, N.G., T.A.S., A.R., Ø.K., T.L., H.H., K.S. and C.B.S.; writing—review and editing, N.G. and T.A.S.; event development and execution, N.G., T.A.S., A.R., Ø.K., T.L., H.H., K.S., C.B.S., T.R., Ø.B. and A.M.S. All authors have read and agreed to the published version of the manuscript.

Funding: This research received no external funding.

Institutional Review Board Statement: Not applicable.

Informed Consent Statement: Not applicable.

Data Availability Statement: Some published results from earlier tests can be found here: https://jammertest.no/publications-findings/ (accessed on 16 February 2026). Please contact the corresponding author for more information.

Acknowledgments: The authors would like to thank the rest of the Jammertest team for all their hard work.

Conflicts of Interest: The authors declare no conflicts of interest.

References

1. EU Agency for the Space Programme. *EO and GNSS Market Report 2024 Issue 2*; EUSPA: Prague, Czech Republic, 2025.
2. Volpe, J.A. *Vulnerability Assessment of the Transportation Infrastructure Relying on the Global Positioning System*; U.S. Department of Transportation: Washington, DC, USA, 2001.
3. Justis- og beredskapsdepartementet. *Digital Sårbarhet—Sikkert Samfunn*; Report from Norwegian Ministry of Justice and Public Security; Justis- og beredskapsdepartementet: Oslo, Norway, 2015.
4. UK Government Office for Science. *Satellite-Derived Time and Position: Blackett Review*; Report from UK Department for Science, Innovation& Technology; UK Government Office for Science: London, UK, 2018.
5. OPSGROUP Team. *GPS Spoofing: Final Report*; Opsgroup: Argonweg, The Netherlands, 2024.
6. Joint Statement by ITU, ICAO & IMO. Retrieved from International Telecommunication. 2025. Available online: https://www.itu.int/en/mediacentre/Documents/2025/ICAO-IMO-ITU-Joint-Statement.pdf (accessed on 12 May 2025).
7. Chew, C.; Roberts, T.M.; Lowe, S. RFI Mapped by Spaceborne GNSS-R Data. *NAVIGATION* **2023**, *70*, 4. [CrossRef]
8. Berz, G. Mitigating GNSS Radio Frequency Interference (RFI). Retrieved from EUROCONTROL. 2025. Available online: https://www.eurocontrol.int/sites/default/files/2025-01/eurocontrol-nmuf-2025-day2-s5-mitigating-gnss-rfi.pdf (accessed on 12 May 2025).
9. Rødningsby, A.; Morrison, A.; Sokolova, N.; Gerrard, N.; Rost, C. RFI Monitoring of GNSS Signals on Norwegian Highways. In Proceedings of the 33rd International Technical Meeting of the Satellite Division of The Institute of Navigation (ION GNSS+ 2020), Online, 22–25 September 2020; pp. 3536–3549. [CrossRef]

10. Nasjonal kommunikasjonsmyndighet (Nkom). *Equipment Failure Causing GPS Reception Denial*; Report from the Norwegian Communications Authority; Nasjonal kommunikasjonsmyndighet: Lillesand, Norway, 2022.
11. Levin, T. Jammertest: The biggest open GNSS vulnerability test in the world. *Mod. Mobil. Og Infrastruktur* **2024**, *2*, 3. [CrossRef]
12. Morrison, A.; Sokolova, N.; Gerrard, N.; Hauglin, H.; Rødningen, T.; Rødningsby, A. Making a Good Thing Better: Jammertest 2023 Jamming, Meaconing, Spoofing, and Synchronization on the Norwegian Coast. *Eng. Proc.* **2024**, *88*, 15. [CrossRef]
13. Morrison, A.; Sokolova, N.; Solberg, A.; Gerrard, N.; Rødningsby, A.; Hauglin, H.; Rødningen, T.; Dahlø, T. Jammertest 2022: Jamming and Spoofing Lessons Learned. *Eng. Proc.* **2023**, *54*, 22. [CrossRef]
14. Knight, R. NAVFEST: As Real as it Gets. Retrieved from Inside GNSS. 2024. Available online: https://insidegnss.com/navfest-as-real-as-it-gets/ (accessed on 12 May 2025).
15. Jammertest. Retrieved from Jammertest. Available online: https://jammertest.no (accessed on 12 May 2025).
16. Jammertest Plan. Retrieved from Github. Available online: https://github.com/NPRA/jammertest-plan (accessed on 12 May 2025).
17. Jammertest—Previous Jammertests. Retrieved from Jammertest. Available online: https://jammertest.no/previous-jammertests/ (accessed on 12 May 2025).
18. Jammertest—Publications & Findings. Retrieved from Jammertest. Available online: https://jammertest.no/publications-findings/ (accessed on 12 May 2025).
19. Testnor. Available online: https://testnor.com (accessed on 12 May 2025).
20. National Aeronautics and Space Administration (NASA). CDDIS NASA's Archive of Space Geodesy Data. Retrieved from NASA Earth Data: CDDIS | | Data and Derived Products | GNSS | Broadcast Ephemeris Data. Available online: https://www.earthdata.nasa.gov/centers/cddis-daac (accessed on 16 May 2025).

Disclaimer/Publisher's Note: The statements, opinions and data contained in all publications are solely those of the individual author(s) and contributor(s) and not of MDPI and/or the editor(s). MDPI and/or the editor(s) disclaim responsibility for any injury to people or property resulting from any ideas, methods, instructions or products referred to in the content.