# Ad Hoc WG on Cyber threats

- Spring of ‘22, the general directors of the nordic NMA’s ordered a report regarding cyber threats.
- An ad hoc working group was established, and work commenced after the summer, aiming for a report delivery in September.
- First delivery, by August 2022 (Notes from delivery description):

| | |
|---|---|
| Powerpoint presentation (duration: 20 minutes) with<br>•Outline of the risks focusing on the future risks (and future GNSS based services) | First delivery.<br><br>Focusing on the risks of both jamming/spoofing and other cyber vulnerabilities of both existing and expected future positioning services. Key words:<br><br>- New applications (Autonomy, drones, mass market applications)<br>- Professional users (High precision, NRTK etc.)<br>- PPP/SSR<br>- CORS safety measures (RF as well as local IT/physical vulnerabilities<br>- IT/Network threats and safety measures |

# Cyber threats to positioning services

## Working group

| Country | Agency | Representative |
|---|---|---|
| Norway (chair) | Kartverket | Tor-Ole Dahlø |
| Iceland | Landmælingar Íslands | Gudmundur Valsson |
| Denmark | Styrelsen for Dataforsyning og Infrastruktur | Casper Jepsen |
| Sweden | Lantmäteriet | Peter Wiklund<br>Kibrom Ebuy Abraha |
| Finland | National Land Survey of Finland | Sanna Kaasalainen<br>Hannu Koivula<br>Topi Rikkinen |

# Presentation outline


- GNSS applications described
  - It is used everywhere!
- GNSS interference threats described
  - Jamming, spoofing, others
- General threats for positioning services
- The impact of GNSS-related cyber threats on the mapping agencies
- Existing monitoring / mitigation measures for GNSS-related threats
  - What is currently being done
  - What is on the market --> what more could be done

- Delimitations:
  - We have recognized IT specific threats, but this is not the main focus of this presentation.
  - GNSS-based timing applications are taken into account, but not looked into in detail in this phase.
    - Timing is critical – and more or less 100% dependent on GNSS

# GNSS is used everywhere:

**Agriculture** – New technologies are pushing the Agriculture sector to new frontiers. GNSS is considered a key driver and enabler for these evolutions, ranging from traditional farming applications to Internet-of-Things, blockchain, Agri-fin tech and value chain management. GNSS-enabled livestock wearables are emerging as an exciting trend which is improving animal welfare.

**Aviation and Drones** – Global air traffic took a huge hit due to COVID-19 – airlines responded with consolidation of fleets, and older aircraft prioritised for retirement. Meanwhile, standards evolution in navigation and surveillance presses ahead, enhanced by growing demand from increasingly sophisticated drone operations.

**Biodiversity, Ecosystems and Natural Capital** – In the domain of biodiversity, ecosystems and natural capital, GNSS-beacons are used to geo-locate animals for the purposes of monitoring migrations, habitats, and behaviours. These are becoming more accurate and additional biodiversity applications are emerging (e.g. botanical mapping).

**Climate Services** – GNSS has limited but important application in the climate services domain. The technology supports a range of geodetic applications that measure properties of the earth (magnetic field, atmosphere) with direct impact on the Earth's climate. GNSS is expected to have an increasing role in the growing market of climate modelling.

**Consumer Solutions, Tourism and Health** – GNSS finds increasing use in facilitating our daily lives. From context-aware apps monitoring peak visit times to contactless deliveries and personal fitness apps (powered by wearable devices), navigation and positioning information plays a vital role.

**Emergency Management and Humanitarian Aid** – Estimated to save 2,000 lives a year, the new MEOSAR system of the GNSS-based COSPAS-SARSAT programme relies on the proper use of GNSS-enabled Search and Rescue beacons. On the field, GNSS is a valuable tool to coordinate emergency response and humanitarian aid.

**Energy and Raw Materials** – Monitoring and management of electricity utility grids heavily rely on GNSS timing and synchronisation, allowing the balance supply and demand and ensuring safe operations. In the domain of raw materials, the increased uptake of augmented GNSS supports site selection, planning and monitoring, as well as mining surveillance activities and mining machinery guidance.

**Fisheries and Aquaculture** – GNSS plays a vital role for the efficient and effective monitoring of fisheries activities through applications such as VMS and AIS. As the focus on the sustainability of these activities grows, agriculture lands diminish and food demand rises, GNSS applications are themselves seeing higher demand.

**Forestry** – GNSS is becoming an extremely valuable tool in monitoring and maintaining the sustainability of our forests. Besides precision forestry management, a key emerging trend is the use of GNSS-enabled UAVs and tracking devices help ensure the health of our trees and the efficiency of our timber supply chains.

**Infrastructure** – GNSS contributes to the proper functioning of Infrastructures operations. It allows a safe and on-time completion of construction work through the provision of high accuracy services and supports the synchronisation of telecommunication networks. With the transition towards 5G, the GNSS Timing & Synchronisation function is expected to play an increasingly critical role in telecommunication network operations.

**Insurance and Finance** – The financial world relies on GNSS timing and synchronisation for the accurate timestamping of financial transactions. Insurers, on the other hand, are turning towards GNSS-enabled UAVs for a more accurate and faster claim assessment.

**Maritime and Inland Waterways** – GNSS has shown its versatility providing data insights to monitor global shipping and port activities during the pandemic. Looking to the future, with automation and 5G expected to bring technological advancements in ports, GNSS will continue expanding its role beyond merely providing navigation information.

**Rail** – GNSS is becoming one of the cornerstones for non-safety related applications (e.g. asset management), whilst future adoption of GNSS for safety-related applications, including Enhanced Command & Control Systems, is expected to increase railway network capacity, decrease operational costs and foster new train operations. Thanks to GNSS taking part in digitalisation, Rail is becoming safer, more efficient and more attractive.

**Road and Automotive** – Despite the global slowdown of car production and sales, regulation for safer and autonomous vehicles is on track, with GNSS doubtless playing a key role. With In Vehicle Systems remaining the dominant source of Positioning, Navigation and Timing, it is moreover clear that public transport is increasingly adopting GNSS to improve its services.

**Space** – From using real-time GNSS data for absolute and relative spacecraft navigation, to deriving Earth Observation measurements from it, GNSS has also proven its worth for in-space applications. Driven by the NewSpace paradigm, the diversification and proliferation of space users leads to an increasing need for spaceborne GNSS-based solutions.

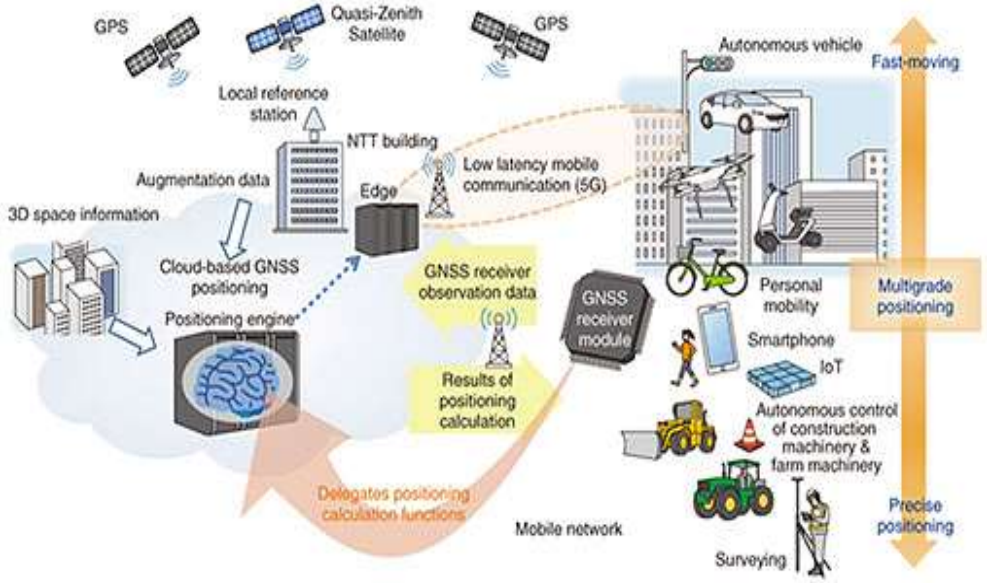
**Urban Development and Cultural Heritage** – In this field, GNSS-based solutions are used, in conjunction with EO, to accurately survey and map urban areas and to build advanced 3D models of the built environment. With more than 56% of the population already living in urban areas and this number expected to increase, digital solutions powered by GNSS will be needed more than ever support sustainable growth.

https://www.euspa.europa.eu/sites/default/files/uploads/euspa_market_report_2022.pdf

# GNSS-based positioning services

For improved accuracy, external data from a positioning service is used. The mapping agencies as well as private service providers offer a range of positioning services:

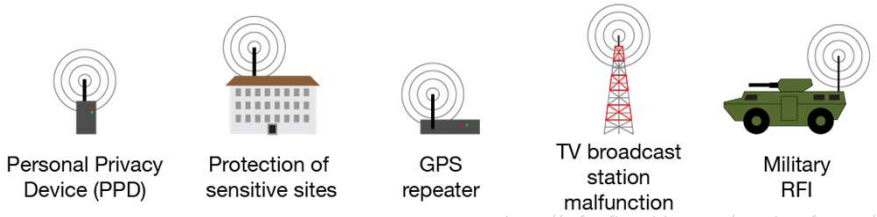
- Network RTK & DGNSS services
  - SWEPOS, CPOS, FINPOS, commercial providers (Leica SmartNet, Trimble VRS Now, TopNet Live etc.)
- PPP / PPP-RTK services
  - Fugro, Trimble RTX, ublox
- Post-processing data from base stations
  - Used for high accuray purposes, both commercial and for geodetic purposes
- Direct data streams from geodetic stations to external service providers



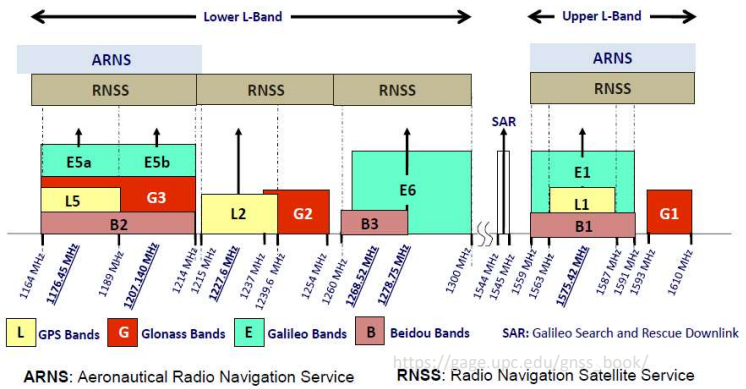

https://www.ntt-review.jp/archive/ntttechnical.php?contents=ntr201906fa3.html)

# GNSS-specific interference threats explained

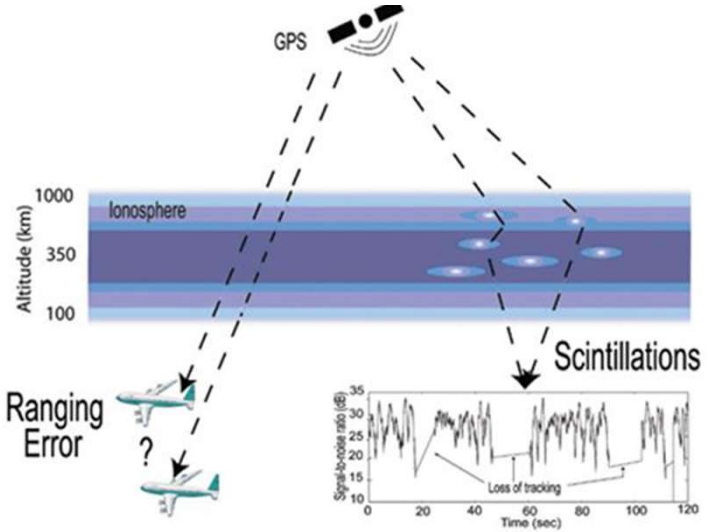
- GNSS signals are transmitted from the satellittes with low power which can easily be disrupted
- Wide frequency bands makes the signals vulnerable to many types of interference
- Increased (un)intentional sources in later years
  - Unintentional interference:
    - Ionospheric scintillations
    - Radio Frequency Interference (RFI)
    - GNSS receiver, antenna malfunctions
  - Intentional
    - Jamming – Disrupts your signal
    - Spoofing – Falsifies your position




https://safetyfirst.airbus.com/gnss-interference/

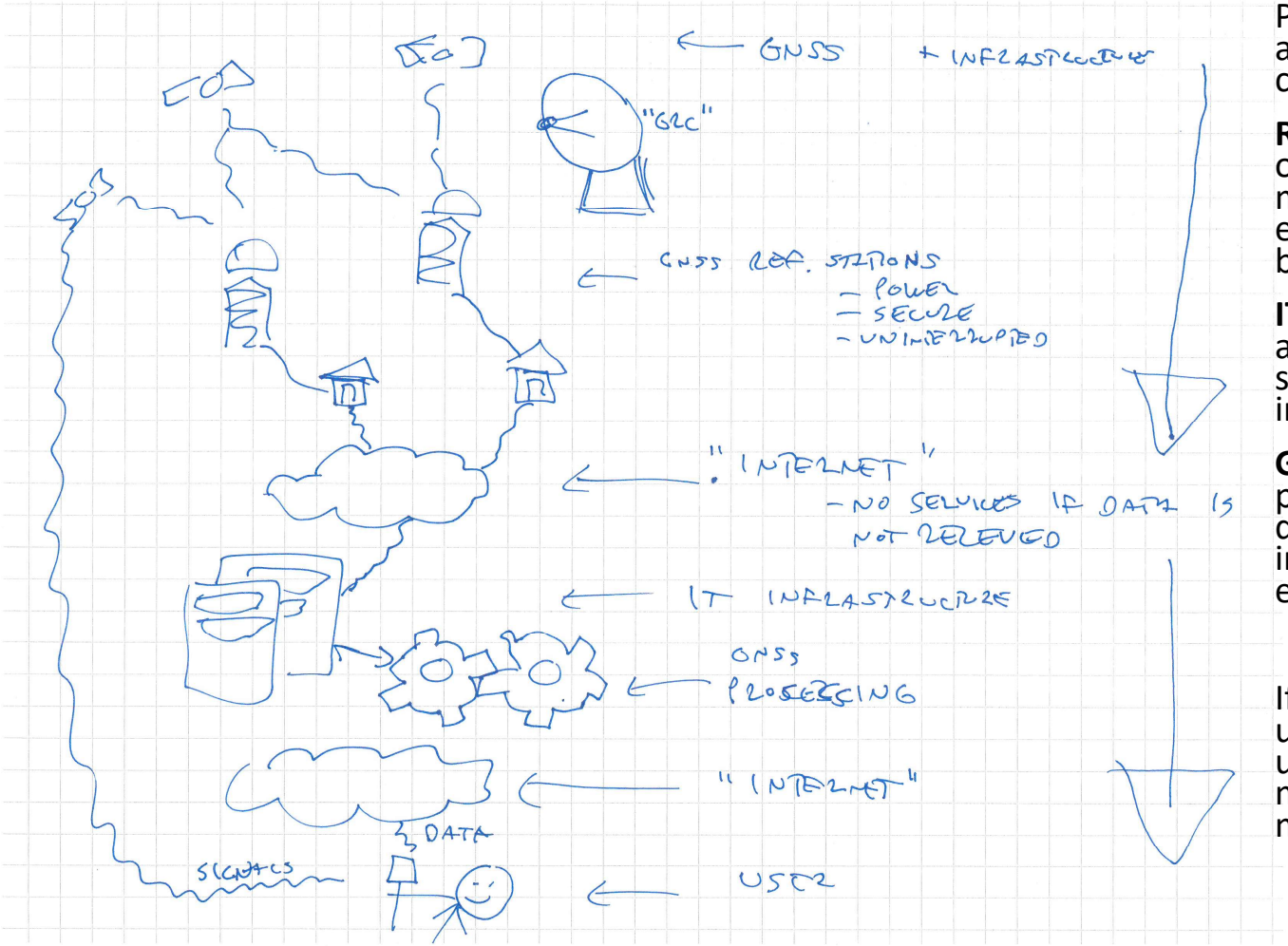



https://gage.unc.edu/gnss_book/




http://www.nap.edu/catalog/12507.html

# Non-GNSS-specific threats for positioning services




Positioning services are complex systems, who are vulnerable to many types of problems and cyber threats. Some examples:

**Reference stations:** Vandalism, power outages, data communications outages (A means to provide the correction data to the end-user. Both internet and satellite-based communications could be disrupted)

**IT infrastructure:** The IT infrastructure of an agency could be attacked, rendering the servers and/or IT network unresponsive or infected.

**GNSS processing segment:** Local GNSS processing systems could be corrupted, either due to IT infrastructure outage or software incidents (sabotage, hacking or operator errors)

If any of these components are rendered unavailable, there is no service for the end-user. Most service providers, including the mapping agencies have built-in redundancy on most of these components.

# Impact on national mapping agencies

- Cadastar work:
  - Positioning services such as Network RTK are widely used for cadastral work
  - Outages on isolated stations, either due to jamming or other outages, does not necessarily impact the availability or quality of the positioning service.
  - Other cyber attacks directed at the main processing facility or the IT network, will have a bigger impact.
- Hydrographical surveys
  - Co-located stations (tide gauges and GNSS) might suffer from jamming/spoofing. Also, hydrographical surveys where real-time positioning services are used for geodetic reference might be affected.
- Geodetic purposes
  - Realizing national reference frames – long outages on critical individual stations might affect high presition time series
  - The quality of national geophysical and atmospheric models could be negatively affected
- Remote sensing application
  - Aerial photogrammetry/laser scanning applications use post-processing data stored by GNSS receivers and the quality could be affected by outages and/or interference.
- Sociatal impacts:
  - Wide-area outages of GNSS has extreme sociatal costs. As more and more end-users in the semi-professional and consumer marked start using positioning services to improve their accuracy, their dependency on the availability and quality of such services increases.
    - LE-IUK-Economic-impact-to-UK-of-a-disruption-to-GNSS-FULLredacted-PUBLISH-S2C190517.pdf (londoneconomics.co.uk)
    - Galileo warning: UK faces £1.7bn a day bill as search for EU replacement 'narrows down' | Science | News | Express.co.uk
    - Bornholmslinjen forsinket to timer: Lastbiler mistænkes for GPS-jamming | Ingeniøren
    - GNSS Jamming: An Omnipresent Threat - Geospatial World
    - Denne kommunen opplever stadig oftere russiske støyangrep • Kommunal Rapport (kommunal-rapport.no)

# Existing monitoring / mitigation measures
(to GNSS-specific threats)

- Monitoring
  - Data analysis
    - Pre-correlation
    - Post-correlation
      - Signal-to-noise monitoring
  - Augmentation (providing information to end-users whether a positioing service or GNSS in general can be trusted or not)
    - Integrity
- Mitigation
  - Mitigation measures on receivers
    - Receiver manufacturers have a big role here
    - Mitigation measures on both base station receivers & rovers (end-user equipment)
    - Jamming test in Norway – Andøya
    - Task force dealing with interference in EGITF (EU GNSS Interference Task Force) - report later this year.
  - Mitigation on antennas
    - Certain antenna types and designs mitigate local jamming/spoofing
    - Antennas are typically installed on rooftops/pillars, and are typically not prone to ground-based interference due to ground planes on antennas
- Physical CORS security
  - Vandalism proofing, reducing the risk of tampering with the installations
  - Physical access to IT hardware on stations: In case of a security breach on the station, the GNSS processing software as well as IT firewalls can disallow unapproved units from gaining access to the rest of the IT network
  - Each institution is doing something, good idea to continue cooperating and sharing experiences

# Future GNSS mitigation techniques

- There are ideas within the Galileo program, but we have no experience yet.
  - Spoofing protection (near-future?)
  - Galileo OSNMA, PRS – will new services offer better protection?

- GPS Chimera - encryption and digital signatures on GPS

- Better mitigation techniques from receiver manufacturers
- More detection capabilities from receiver manufacturers & GNSS software

# Future recommendations

- It is recommended by the working group that this topic is continued also after delivering these reports.
- Organization: A task force managed by the mapping authorities themselves.
- This group in relation to the EU task force (EGITF, EU GNSS Interference Task Force)
  - At the moment it is unclear who is involved in the EU task force. What will potentially be the relation with a Nordic initiative? It is recommended to keep this task force as a local, independent initiative.
- Future topics for a Nordic task force on cyber threats:
  - Sociatal impacts
  - Cadastral impacts
  - IT specific threats

# Ad Hoc WG on Cyber threats

- The first report was delivered august ‘22, and the feedback was positive.
- Second delivery was scheduled for spring 2023, but needed to be postponed. The second and final delivery was made autumn 2023, from the following delivery description:

| | |
|---|---|
| Powerpoint presentation with (duration: 20 minutes)<br>•Catalogue of possible mitigation actions in answer to the risks<br>•Evaluation of potentials and barriers/costs | Second delivery, specification after feedback from first meeting. |

Cyber threats to positioning services

Second report: Mitigation actions and the way forward

# Cyber threats to positioning services - Working group

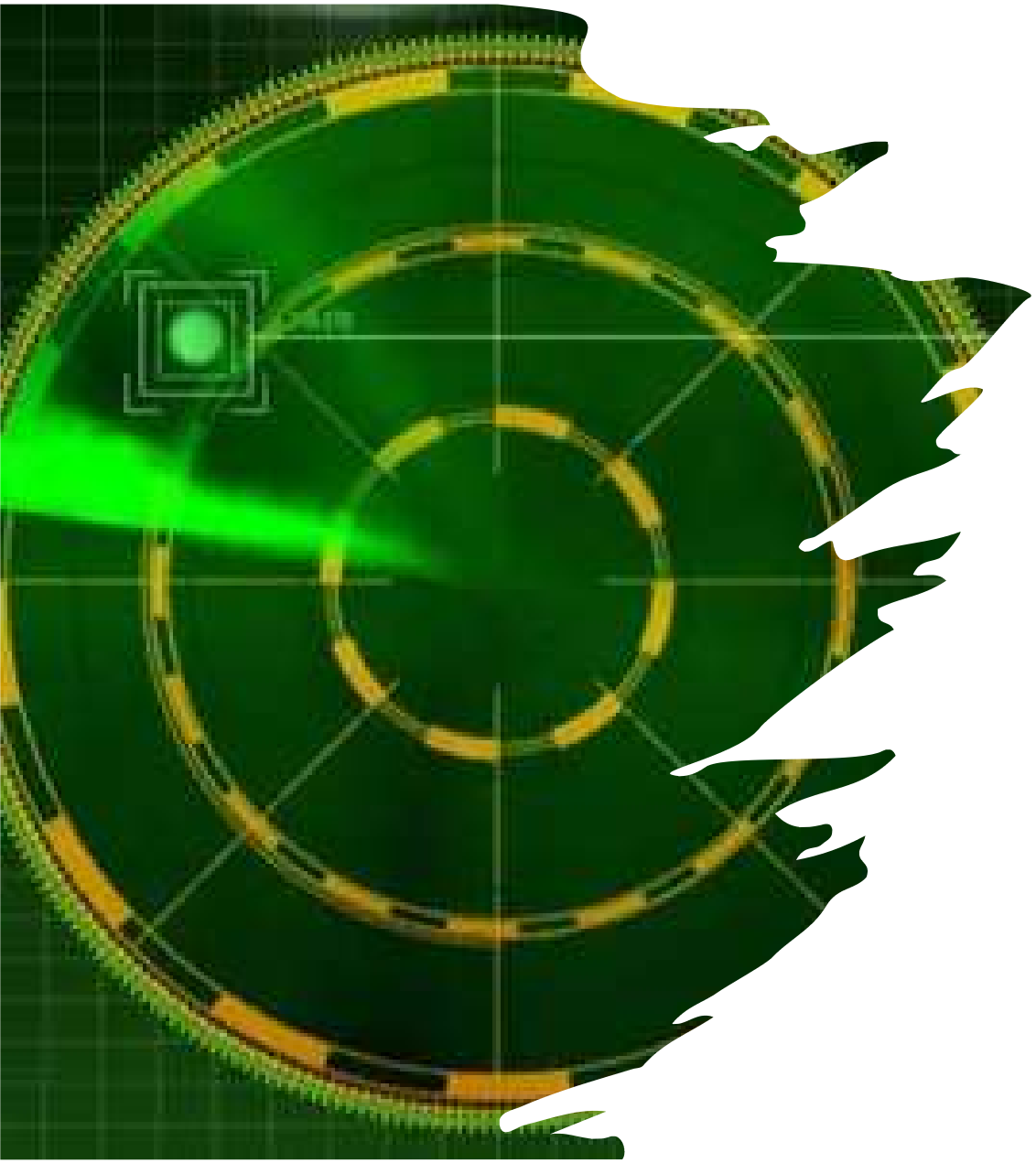
| Country | Agency | Representative |
|---|---|---|
| Norway (chair) | Kartverket | Tor-Ole Dahlø |
| Iceland | Landmælingar Íslands | Gudmundur Valsson |
| Denmark | Styrelsen for Dataforsyning og Infrastruktur | Casper Jepsen |
| Sweden | Lantmäteriet | Peter Wiklund<br>Kibrom Ebuy Abraha |
| Finland | National Land Survey of Finland | Sanna Kaasalainen<br>Hannu Koivula<br>Topi Rikkinen |

# Presentation outline

- Summary of first report
- General on the challenge of interference detection
- Active initiatives
  - Detection
  - Mitigation
  - Co-operation initiatives
- Recommendations

# Summary of first report

- GNSS usage explained
- Overview of existing positioning services in the mapping authorities as well as private service providers
- GNSS-related cyber threats explained
  - Intentional and un-intentional disturbances
  - Jamming and spoofing
- Non GNSS-specific cyber threats such as IT vulnerabilities
- What could the impact of both GNSS-related and other cyber threats be on the national mapping agencies
- Existing monitoring and mitigation measures
- Future GNSS mitigation techniques



# The challenges of interference detection

- The problem:
  - GNSS receivers receive very weak satellite signals, which can be overpowered by other radio sources in the same frequency band.
  - There is always a certain noise/interference level that a GNSS receiver has to deal with.
  - The receivers are in a normal situation very good at filtering out and retrieving the authentic GNSS satellite signals from the noise.
  - When the power level of a jammer or a spoofer exceeds the receiver's ability to find the true signal, the receiver is jammed/spoofed.
  - One isolated GNSS receiver has little awareness of where or what the interference is coming from. It simply is not able to pick out the geniune satellite signal since it is hidden in the noise and/or overpowered by a false signal.
- On the upside:
  - Serious threats like targeted governmental and/or military jamming rarely affect the base stations, due to their nature; Such jammers are very high powered but are typically placed quite far away. Therefore a high powered jammer's signals are typically found at higher elevations, and the GNSS receivers in the CORS network typically benefit from the natural topography shielding them.
  - Jamming from consumer type units are more common, but less of a threat as they typically are very local, intermittent and significantly weaker.

# Active initiatives – Monitoring and security

- On GNSS receivers:
  - Signal-to-noise monitoring: Comparing the GNSS satellites signal strength to normal values, in order to reveal false signals.
  - State of the art geodetic GNSS receivers are able to detect abnormal power levels and interpret these correctly as jamming.
- System level:
  - Using signal to noise levels from older/legacy receivers to detect abnormal values within a detection system. SWEPOS is doing work on this.
  - Using other services such as ionosphere monitoring systems to rule out natural disturbances as the interference source.
- Augmentation
  - Integrity: Providing information to end-users whether a positioning service or GNSS in general can be trusted or not. This can be done using monitoring stations.
- Physical security
  - Vandalism proofing, reducing the risk of tampering with the installations.
- IT security
  - Physical access to IT hardware on stations: In case of a security breach on the station, the GNSS processing software as well as IT firewalls can disallow unapproved units from gaining access to the rest of the IT network.
  - The use of encrypted lines and authorization in the data transfer from the GNSS stations to the central processing facility is becoming the new standard.

# Active initiatives - Mitigation

- Measures on receivers
  - Increased focus and attention on interference detection and mitigation at the manufacturer side.
  - Automatic and dynamic measures on the receivers, such as increased antenna gain when the general noise levels are raised.
  - Possibility to filter out parts of the GNSS spectrum which are disturbed, i.e. masking out the interference signal.

- Mitigation on antennas
  - Certain antenna types and designs mitigate local jamming/spoofing
  - Antennas are typically installed on rooftops/pillars, and are typically not prone to ground-based interference due to ground planes on antennas.

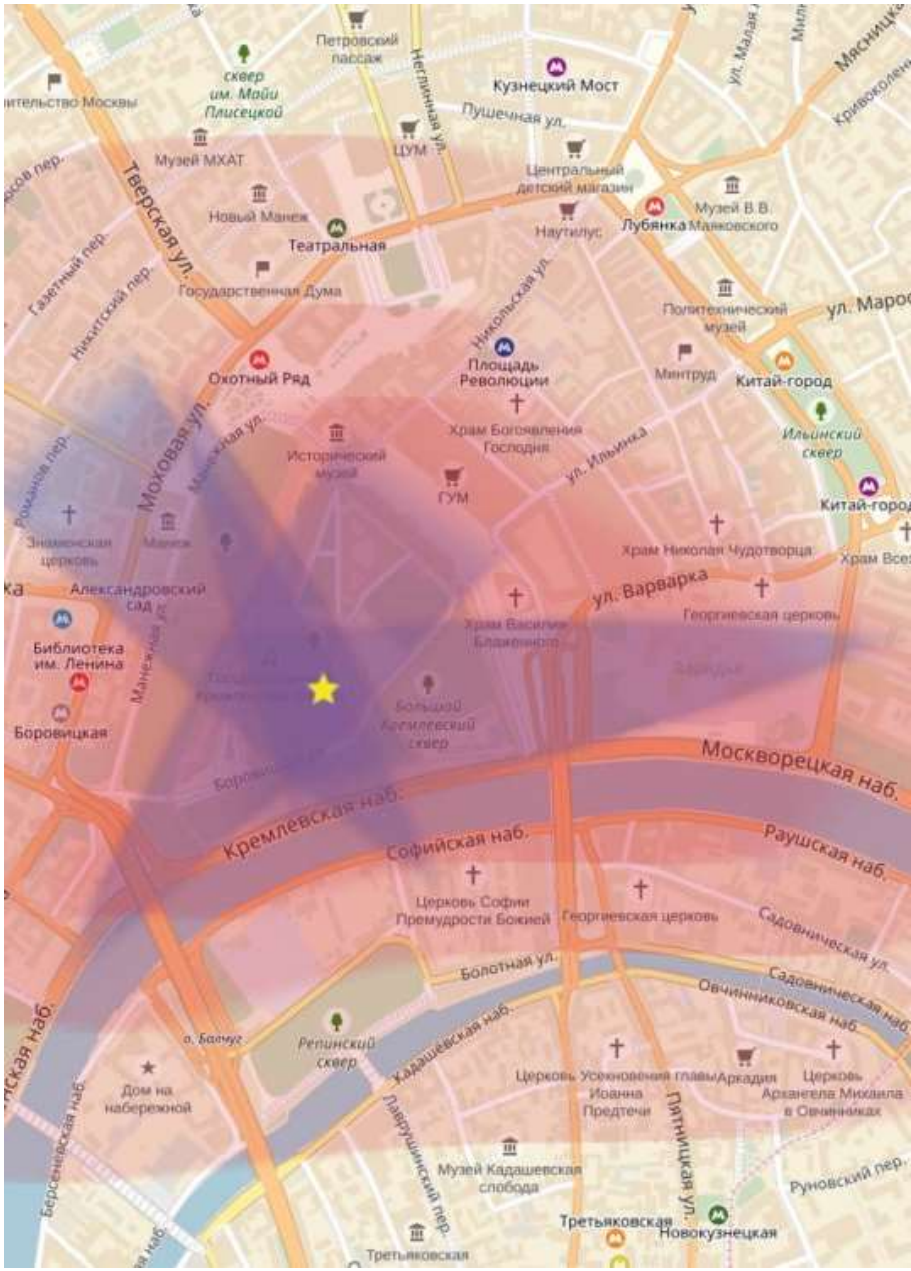
- Mitigation on the system / position service level:
  - Single affected base stations are commonly automatically removed from the positioning services when jammed/spoofed. In case of jamming, the CORS simply is unable to provide data. Spoofing is detected when the CORS position changes, and is also commonly excluded when its calculated position differs from its true position. Positioning services as a whole are quite robust against these threats.

# Active initiatives

- Co-operation initiatives
  - NKG Working group on GNSS – Collaboration and knowledge exchange.
  - Collaboration between authorities on national level, such as road, space and communication authorities.
  - Representatives from the NMA's participate on Jammertest in Andøya, Norway
  - Task force dealing with interference in EGITF (EU GNSS Interference Task Force) - report expected in 2023.
  - Each institution is doing something, so it is a good idea to continue cooperating and sharing experiences!

# Future GNSS mitigation techniques

- Authentication services:
  - Galileo OSNMA, PRS – will new services offer better protection? OSNMA verification of signals is already available in some receiver types, but more knowledge and testing is required.
  - GPS Chimera - encryption and digital signatures on GPS
- More detection capabilities from receiver manufacturers & GNSS software
  - We see that receiver manufacturers provide more and better detection capabilities, both on the receiver level and at a system level.
- Co-operation with communication authorities with has a huge potential!
- Reduce the number of consumer grade jammer units in the public:
  - Legislative and communication authorities' responsibility.
  - However, they need input and detection capabilities from the NMA's.



# Recommendations and summary:

- The mapping authorities need to continue collaborating on this issue. There is already a working group within the Nordic Geodetic Commission with participants from all relevant countries who has this topic on the agenda.
- The service providers of positioning services, be it governmental or private, already mostly use state-of-the art receivers and software which are quite resilient to severe consequences of jamming and spoofing. Still, one can recommend that the geodetic infrastructure should continue to be built and maintained with robustness and resilience to interference and physical interventions in mind.
- The mapping authorities should take advantage of their infrastructure and detection capabilities, and make their data and analysis reports available to the correct authorities, i.e. the communication authorities.

# Ad Hoc WG on Cyber threats

- Final summary and feedback from the DG’s was:

E-mail received November '23:

...

"The first report was presented in our Nordic meeting in 2022 and the 2nd report was presented in September this year.

The conclusion on this agenda item from this year's meeting was the following:

...the work in the Cyber Threats group chaired by Tor-Ole Dahlø. Based on the report he pointed out, that the service providers of positioning services, be it governmental or private, already mostly use state-of-the art receivers and software which are quite resilient to severe consequences of jamming and spoofing – but it continues to be important for geodetic infrastructure to be built and maintained with robustness and resilience to interference and physical interventions in mind.

Furthermore, the mapping authorities should take advantage of their infrastructure and detection capabilities, and make their data and analysis reports more easily available to the telecom authorities.

**The recommendation is, that mapping authorities must continue collaborating on this important issue, and this can be done in a working group within the Nordic Geodetic Commission.**

The reports were acknowledged, and DG’s positions on the way forward and the issues raised, were referred to the DG’s meeting for further discussion and decision:

Regarding Challenge B - Cyber threats:

**The DG’s decided to endorse a handover of the continued investigations to the NKG network. "**

...