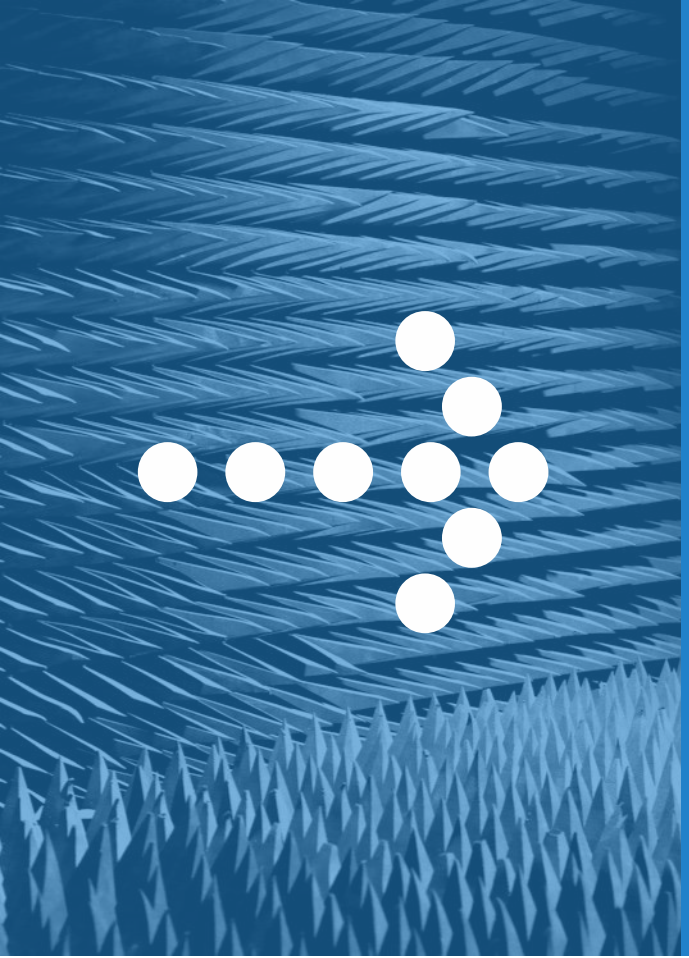


STRIKE3 – En resumé av vad som gjorts och vad vi har hittat

Mikael Alexandersson, Robust Telekommunikation
e-post: mikael.alexandersson@foi.se

FOI

Varför ska vi mäta i GNSS-bandet?

- GNSS är idag en viktig del av vår kritiska infrastruktur
  - finanssektorn, energisektorn, värdetransporter
  - telekom, radio/TV
- Förbjudet att sända och inneha störsändare
- På sikt krav på de länder som ska använda Galileo
- Flertal incidenter finns rapporterade
  - USA, Storbritannien
  - Sverige (indirekt)
- Billigt och enkelt att bygga/köpa störsändare
- ”Personlig Integritet”… (PPD)

Hot och incidenter

3000 kr

200 kr…

N.J. man fined $32K for illegal GPS device that disrupted Newark airport system (8 Aug 2013)

Forskningsfrågor

- Hur upptäcker vi en incident
  - Allt som sticker upp över bruset är misstänkt
- Allt som detekteras påverkar inte alltid GNSS
- Svårt och kostsamt att lokalisera emittrar (ex Newark 18 mån)
- Klassificering önskvärt
  - CW, Chirp, brusstörning
  - hotbibliotek
  - vad är ”värt” att spara
- Lokalisering
  - Hur hittar vi bekymren (rent fysiskt)

STRIKE3

Standardisation of GNSS Threat reporting and Receiver testing through International Knowledge Exchange, Experimentation and Exploitation

Project homepage: http://www.gnss-strike3.eu/

FOI

Sju projektpartners

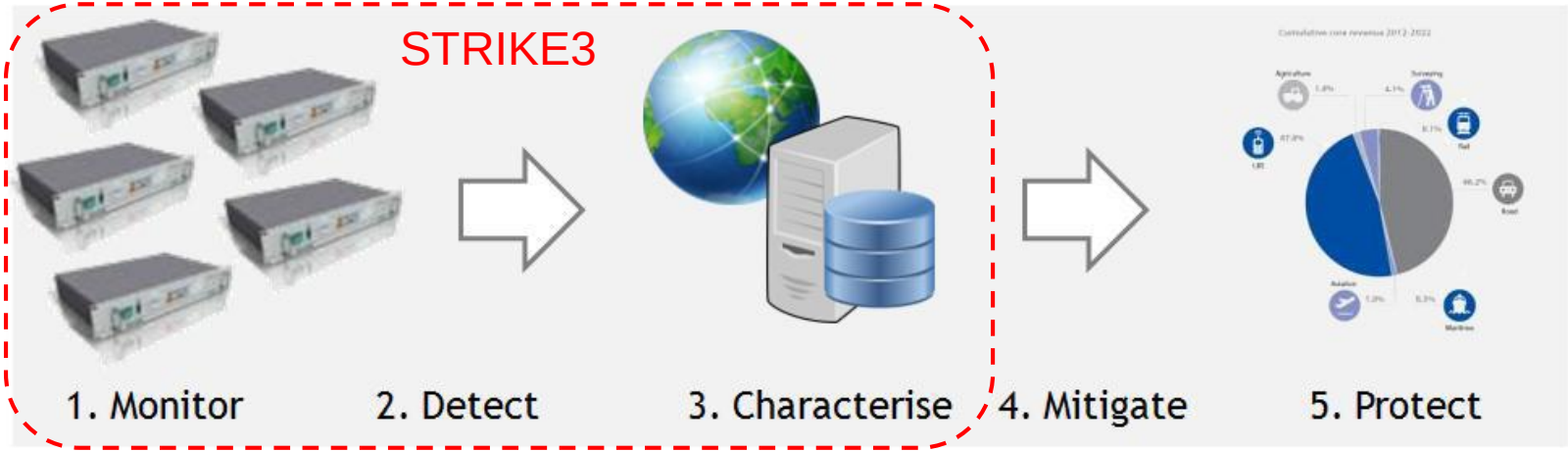
- NSL (Coordinator), UK
- FOI, Sweden
- NLS/FGI, Finland
- AGIT, Germany
- SAC, UK
- GNSS Labs, India
- ETRI, Republic of Korea

STRIKE3 Project

- The STRIKE3 project has been awarded by the European GNSS Agency (GSA) within the Horizon 2020.
- Develop and validate new international standards for monitoring, reporting and testing of GNSS threats.
- STRIKE3 does not attempt to identify, locate and resolve the source of the interference and jamming transmissions.
- Duration: 3 years (1. Feb. 2016 to 31.01.2019)
- Budget: 1.3 MEuro (FOI ca 2 Msek)

FOI

Projektmål


STRIKE3
1. Monitor
2. Detect
3. Characterise
4. Mitigate
5. Protect

State of the Art Review

Considered various aspects

- Stakeholders, causes of threats, existing systems and test benches, existing standardisation activities, etc.

“GNSS Threat Monitoring and Reporting: Past, Present, and a Proposed Future”

Journal of Navigation, Volume 71 Issue 3

Producerade dokument

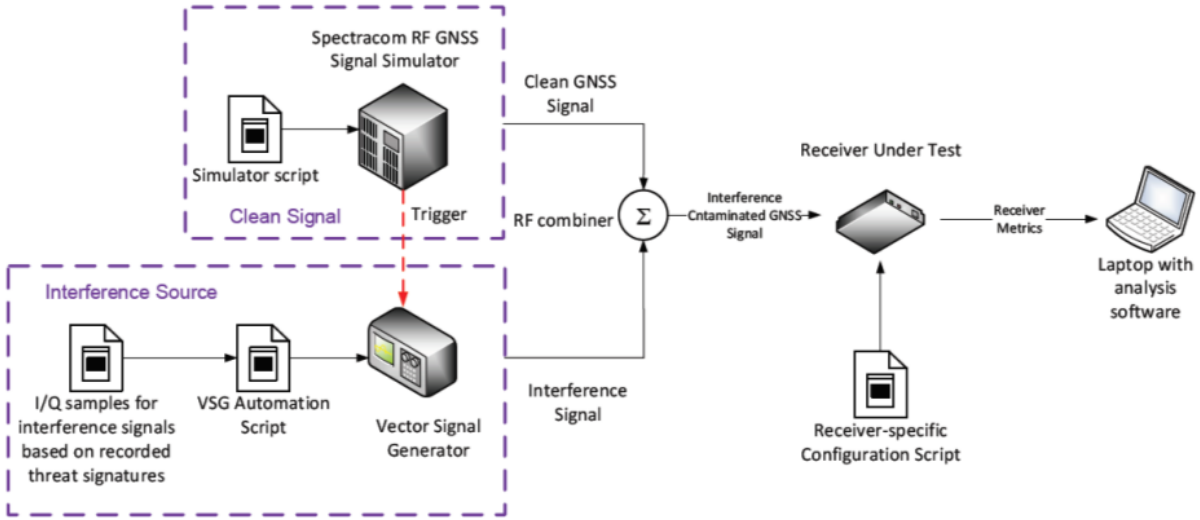
- Rekommendationer (inte standarder…)
  - “Draft Standards for Threat Monitoring and Reporting”
  - “Draft Standards for Receiver Testing Against Threats”

KNOWLEDGE EXCHANGE

- 11 papers
- 8 journals
- 22 conferences/workshops all over Europe; USA, various Asia, Australia
- Invited presentations
  - US DHS meeting
  - United Nations ICG
  - US PNT Advisory Board
  - EUROCONTROL / ICAO
  - IAIN

Mottagartestning

- Lab tests based on simulated GNSS signals
- Interference signals added to clean GNSS signals
- Tested variety of receivers
  - Public report will be available at end of project (Jan 2019)



Interference detection equipment

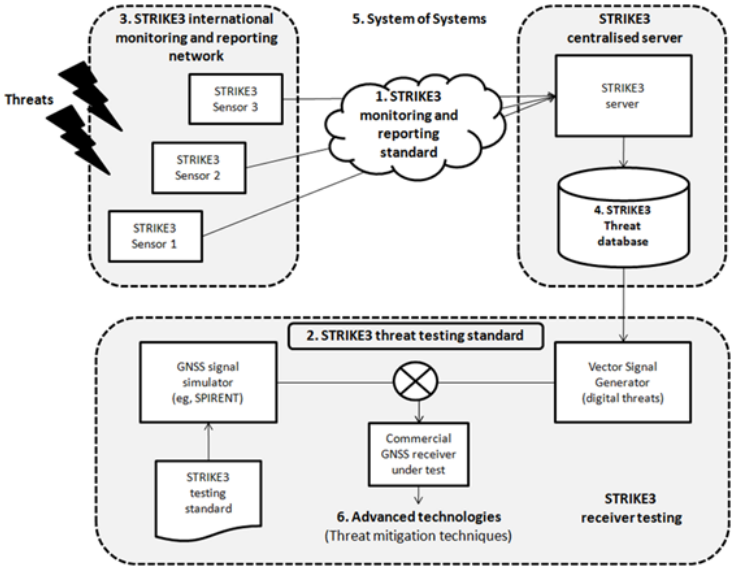
GSS 100D (NSL)
RF Oculus (FOI)

- Software defined radio (SDR)
- COTS GNSS receiver (Civil GPS L1)
- Computer with HDD storage
- Measures power continuously
- Store relevant measures (power, C/N_0, time, position etc.) when thresholds are exceeded
- Network connection to server

FOI

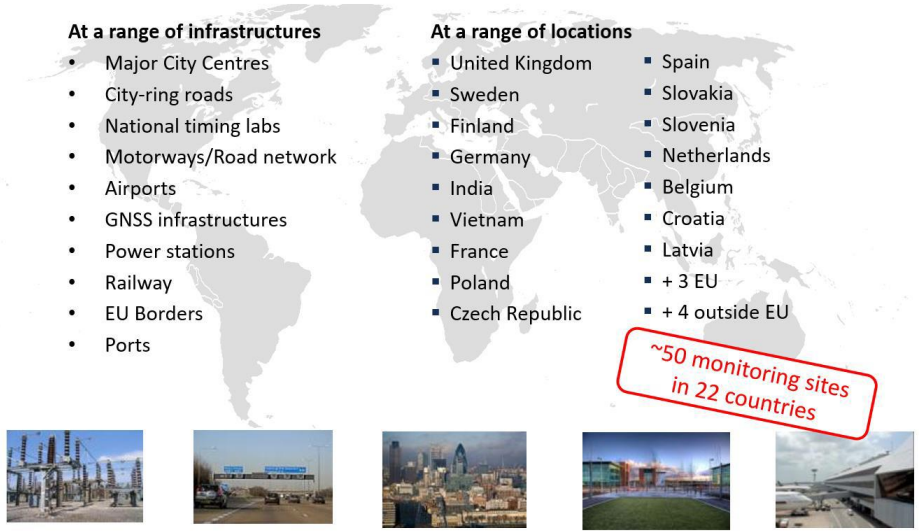
Back-office server and database

- Network connection to nodes
- Receive, collect and store events
- Classification of events
- Web interface for accessing data



Ett år av mätningar

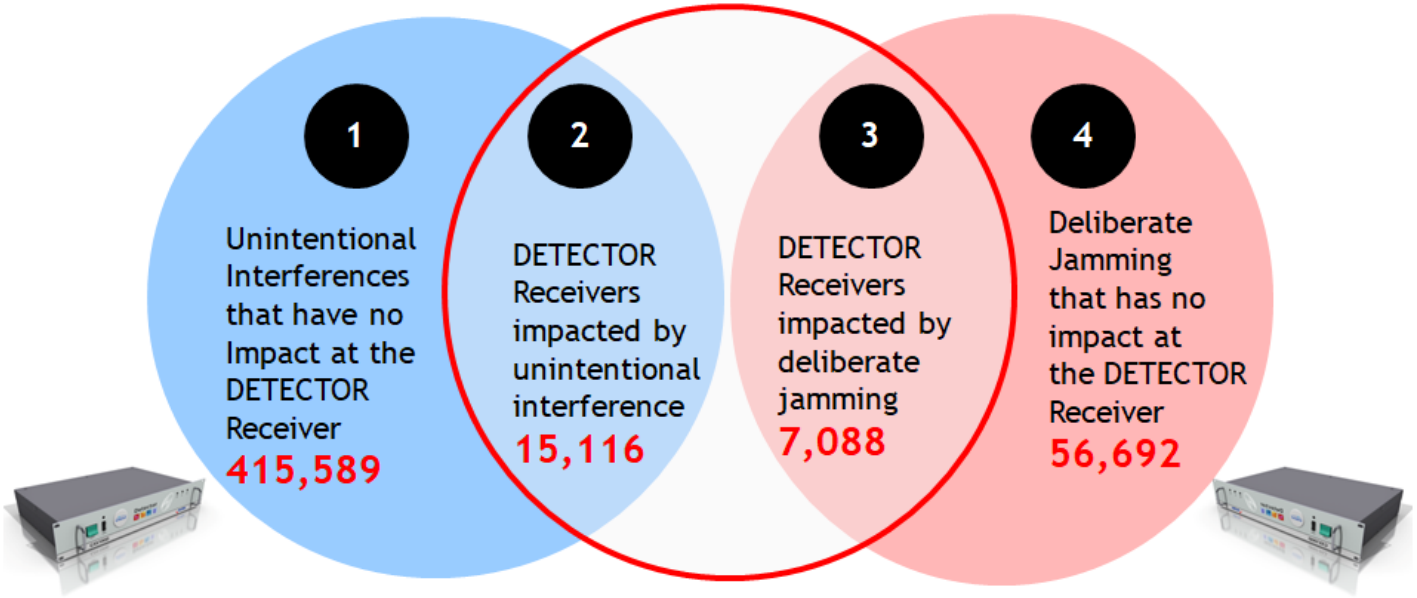
- Monitoring from International Network for 1 year (more for some sites)
- Various equipment reporting to central database for analysis



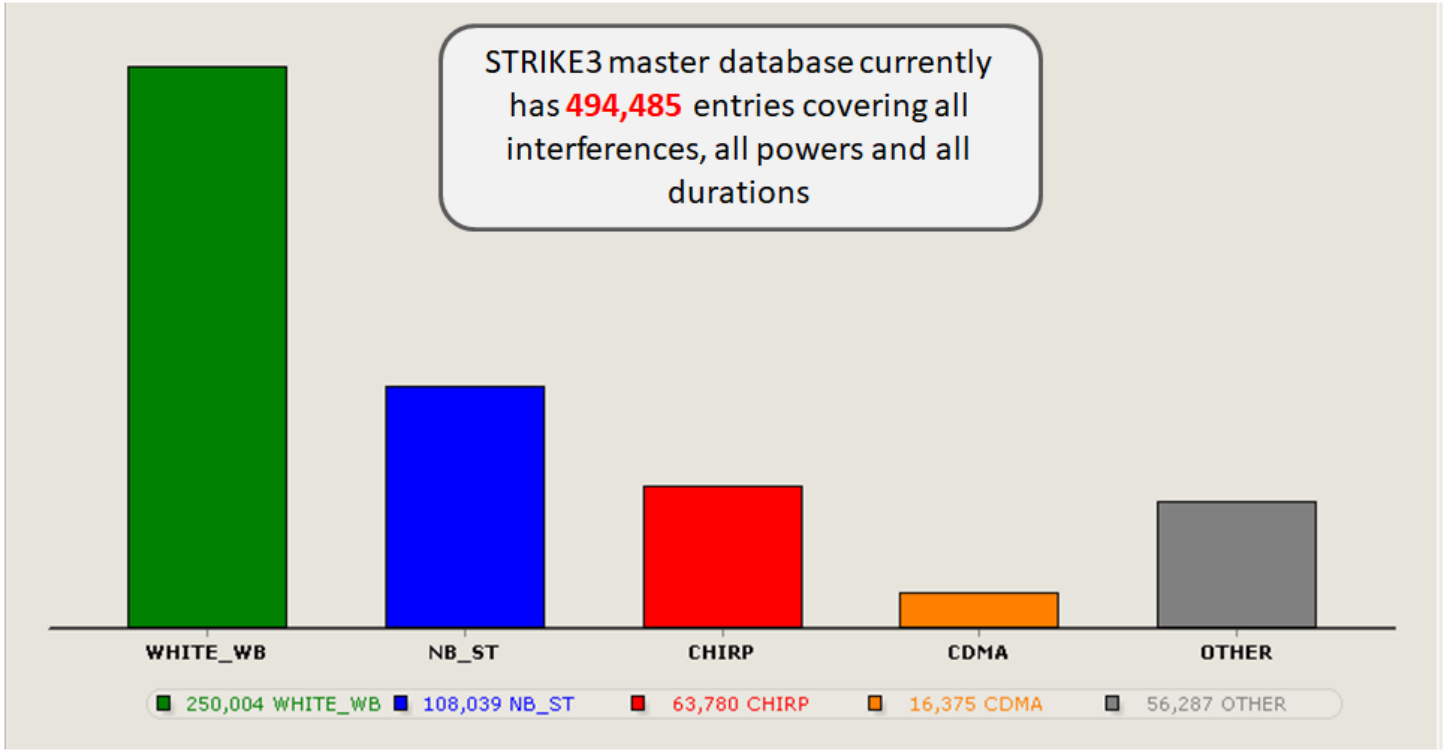
We failed to get into a Bank!

FOI

Sammanfattning av detektioner



Databas (1/2/2016 – 31/10/2018)

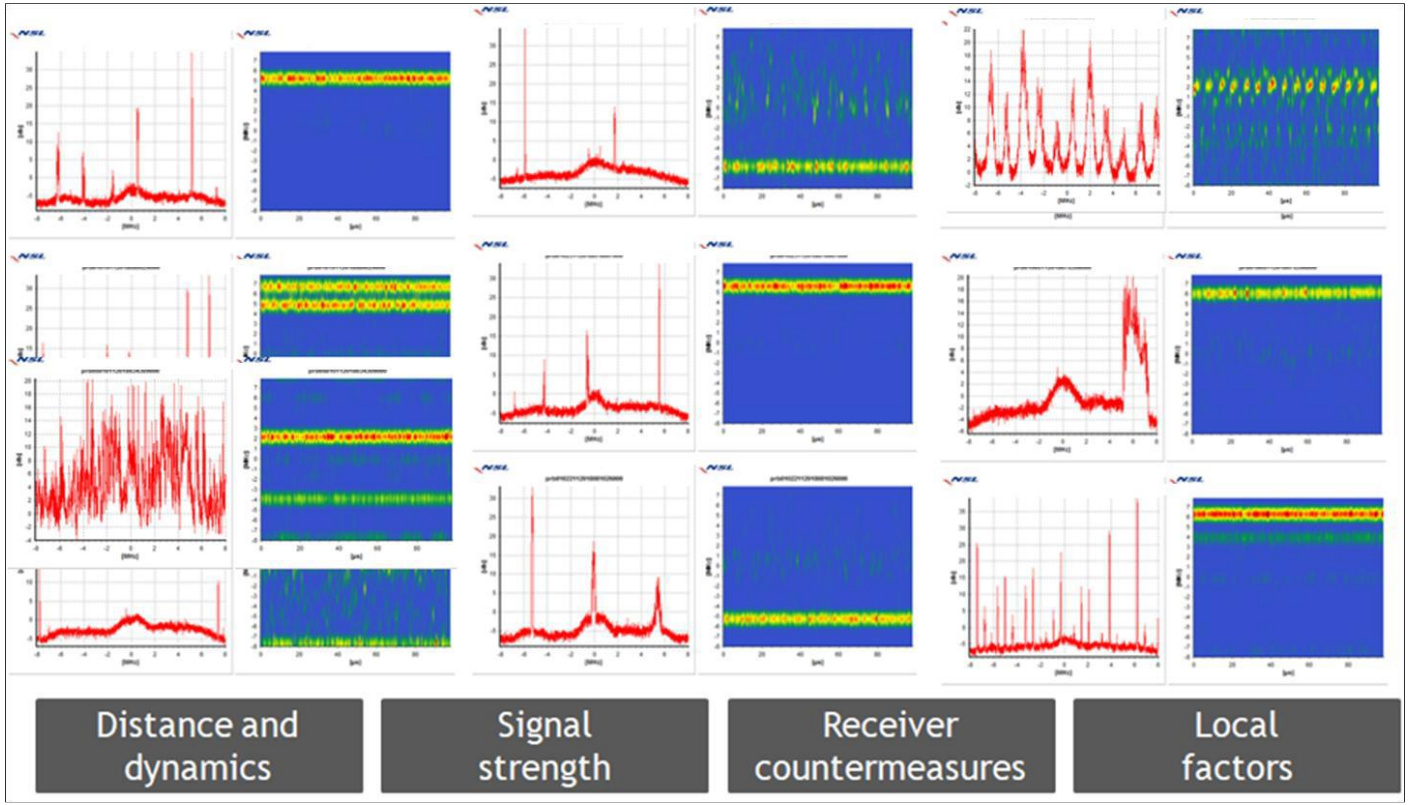


Incidenter

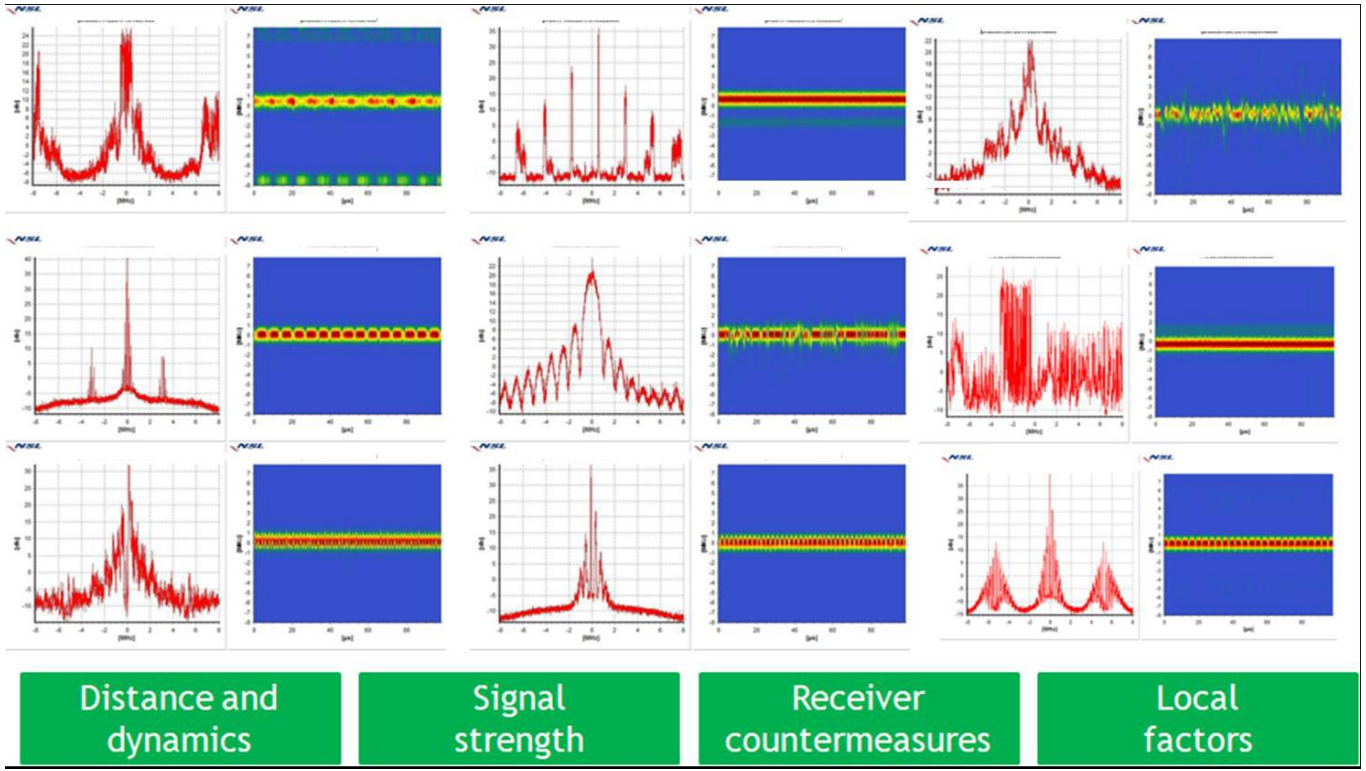
Some findings:

- 7191 events > 5 minutes
- 1112 events > 30 minutes
- 610 events > 60 minutes
- 5 events > 1 day
- Longest event = 5 days

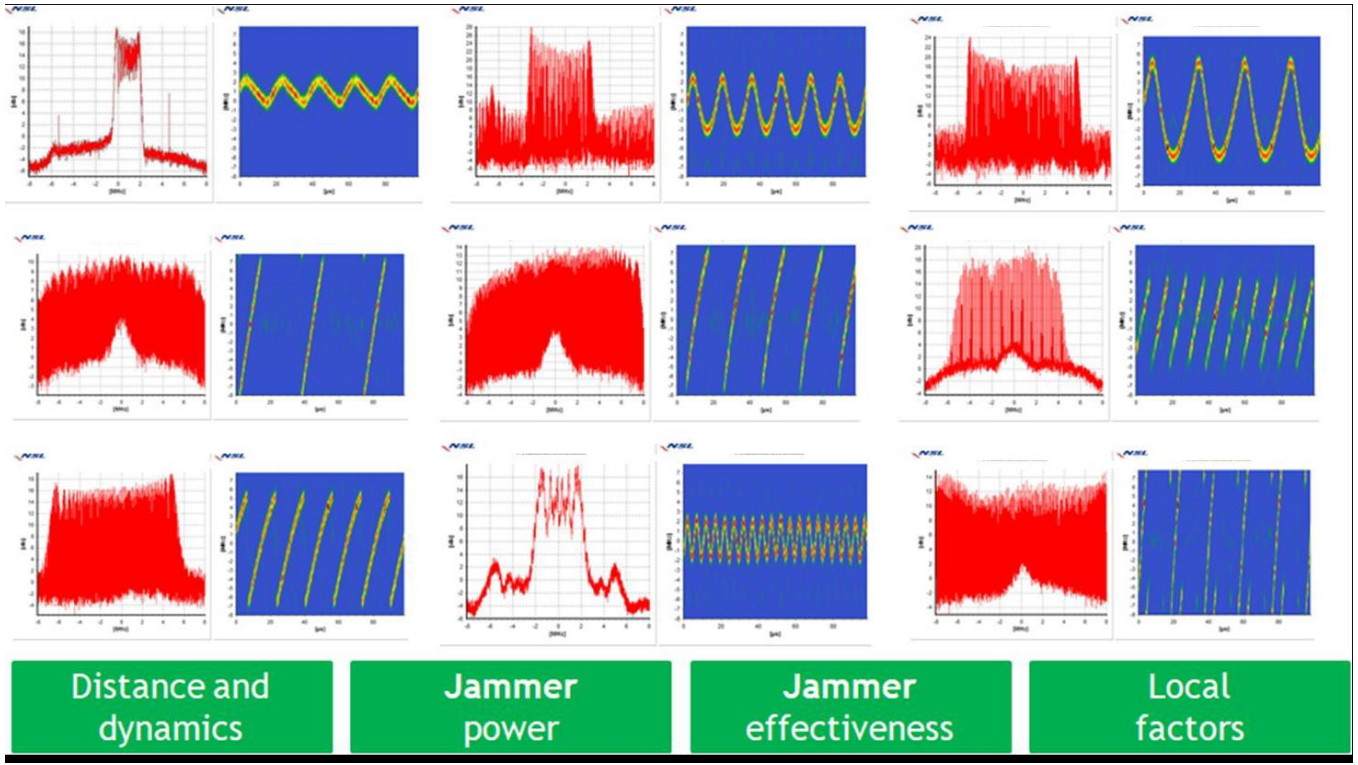
415,589 interferences that did **not** deny GNSS



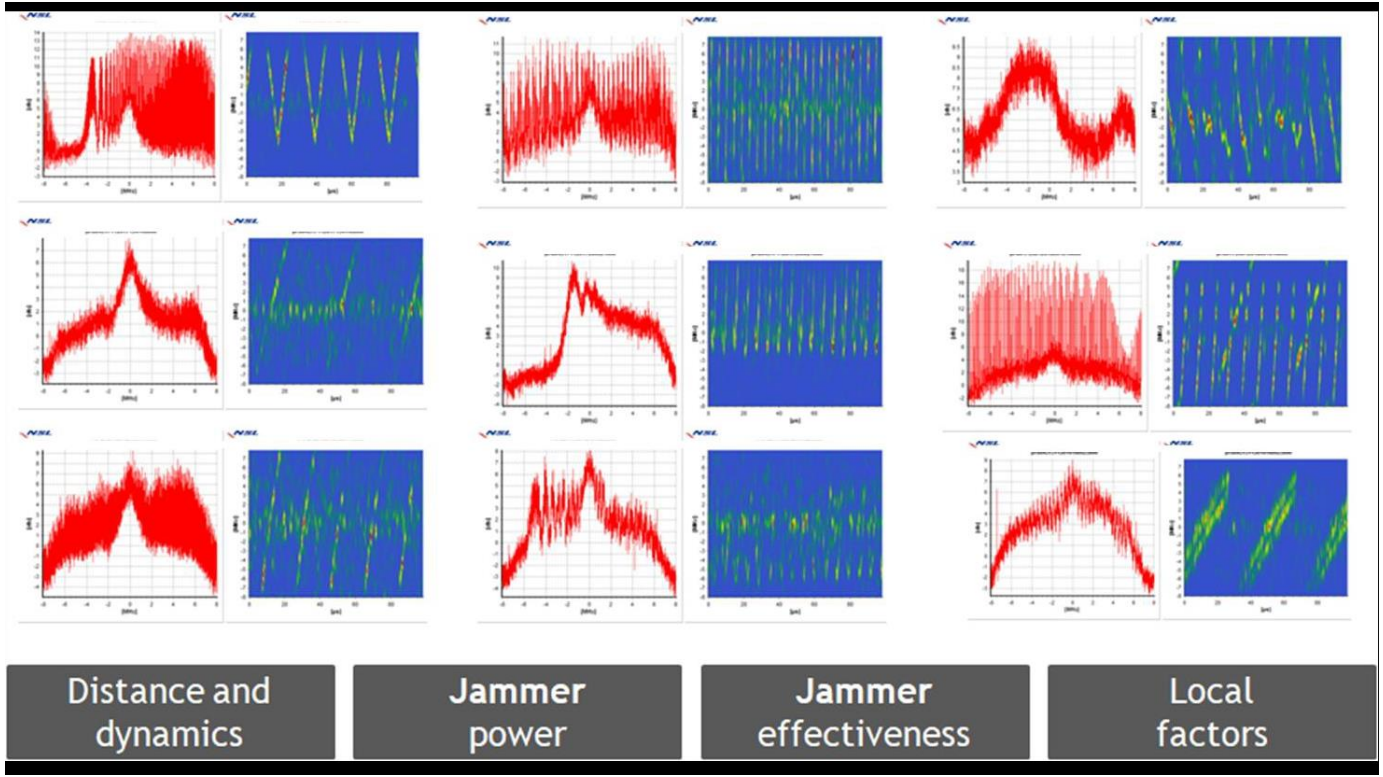
15,116 “interferences” that **denied** GNSS



7,088 jammers that **denied** GNSS



56,692 jammers that did **not** deny GNSS



STRIKE3 site comparisons – mix of interferences

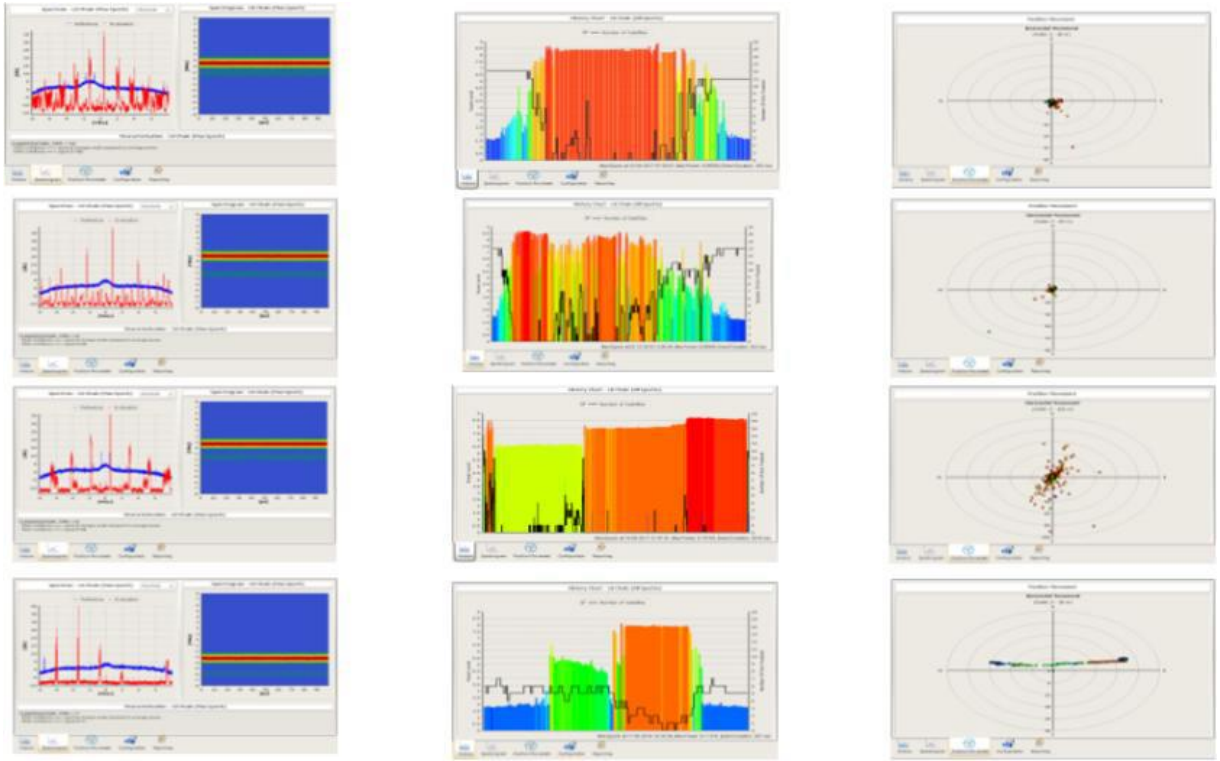
Results from **8 Airport installations**
Most are “national” airports. Most are **air-side** installations.
30 days data (may not be the same 30 days)

	RFI events	Jammers	Jammer/events ratio	Duration > 60secs	GNSS denial	Denial/events ratio
National Airport	8716	95	1%	282	362	4%
National Airport	759	27	4%	200	211	28%
National Airport	2764	595	22%	395	753	27%
Regional Airport	556	31	6%	6	95	17%
National Airport	904	168	19%	158	182	20%
National Airport	776	19	2%	101	35	5%
National Airport	1819	73	4%	9	252	14%
National Airport	4519	133	3%	352	153	3%

Helps to diagnose issues with unintentional interference & jamming
Helps to compare with other sites

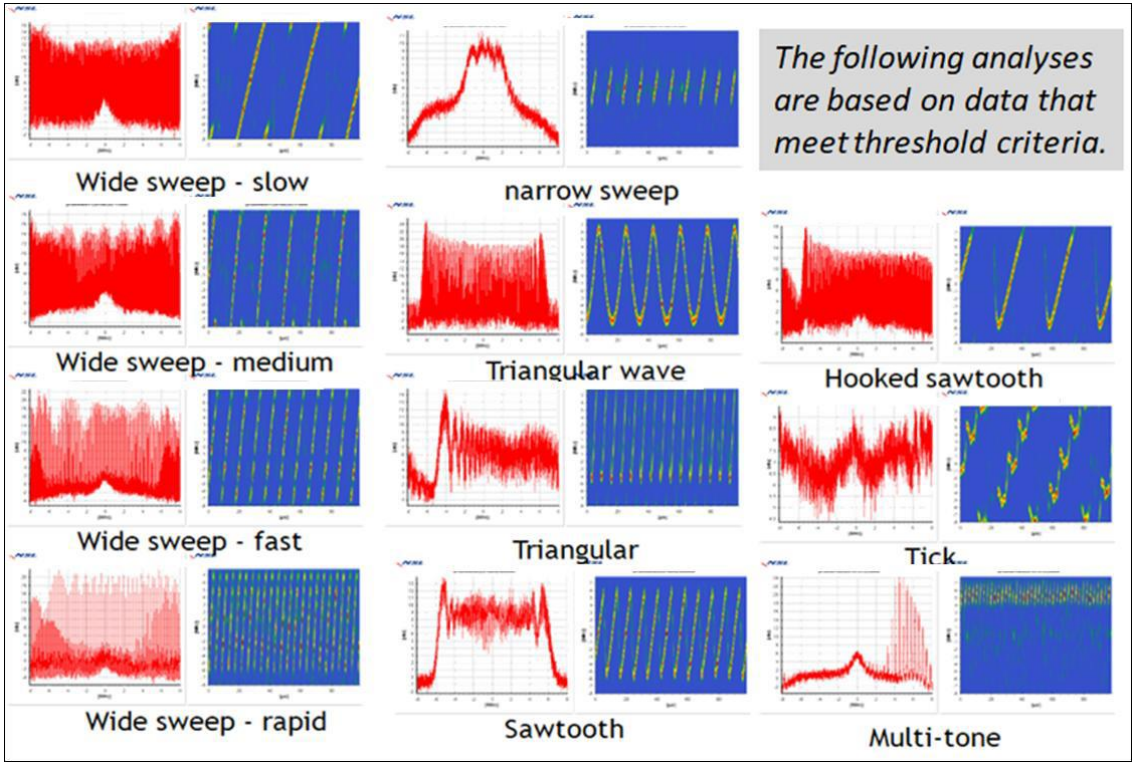
FOI

Påverkan från icke-avsiktliga interferenser

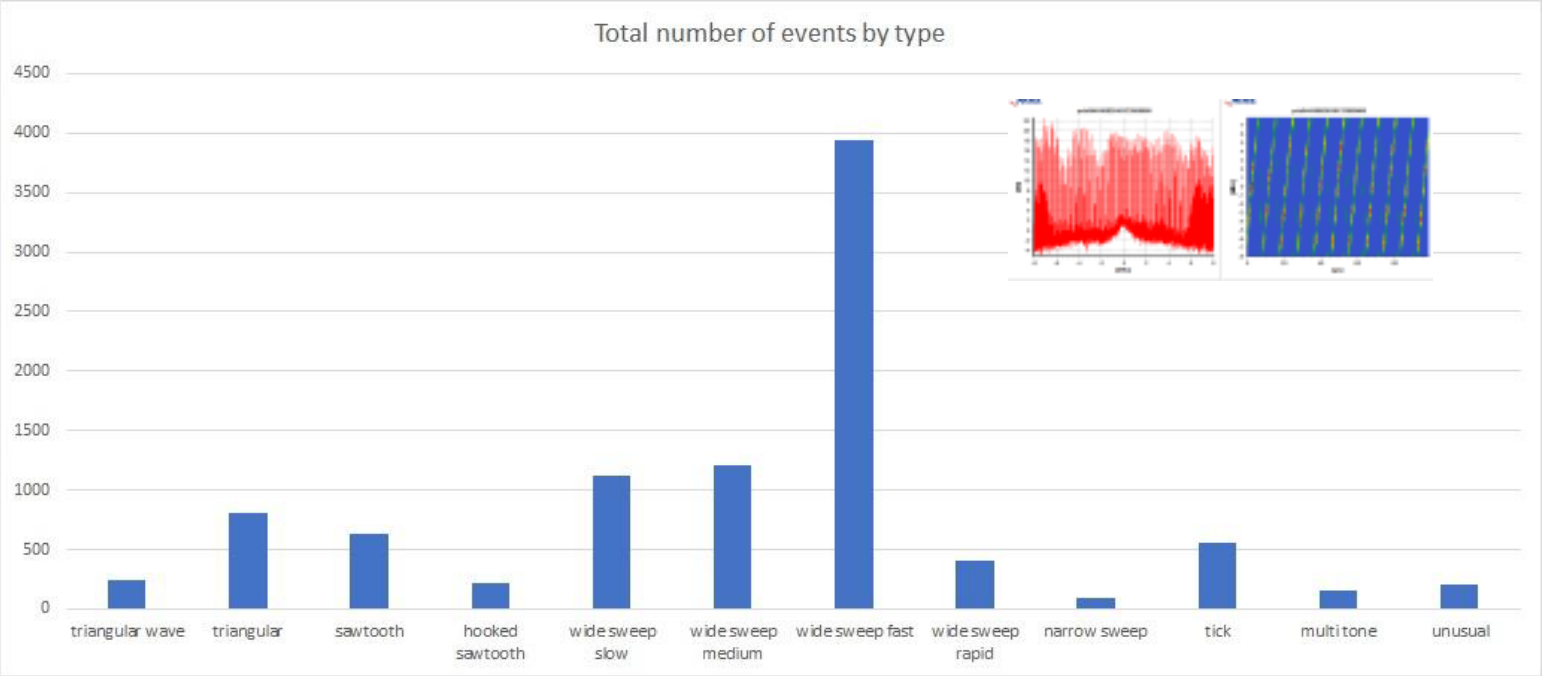


Positionsfel på hundratals meter!

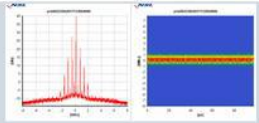
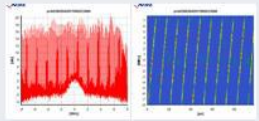
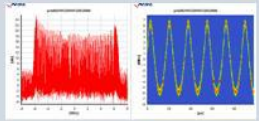
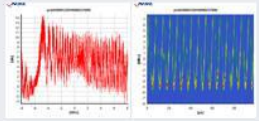
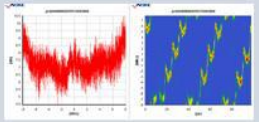
Olika typer av störsändare…



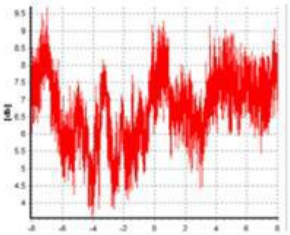
”Populäraste” störsändaren

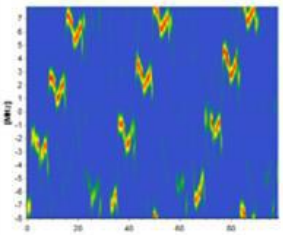


Testsignaler för mottagartest

Type of signal	Example Plots	Reason for choice
Narrow band on L1		Example unintentional(?) signal – this type seen on multiple occasions and at multiple sites
Wide Sweep – fast repeat rate		Very common (total number of events, and number of sites)
Triangular wave		Common (and number of sites)
Triangular		Common (and number of sites)
Tick		Increasingly common. Evolving threat (new type).

Teknikutveckling…





Waveform detected at 4 STRiKE3 sites Europe and outside EU

2017

2017

USB L1/L2 jammer

2018

OBD “covert” jammer

FOI

Sammanfattning

- No reported incidents of loss of GNSS from our stakeholders during the monitoring campaign, despite the amount of interference
- Far more RF Interference than expected
  - GNSS users are accepting/tolerating losses
- Many more RF interferences than jammers
  - 500,000 events (70,000 jammers)
- Many more jamming events than expected
- Many more jammer waveforms than ever expected
  - bandwidths, centre frequencies, chirp rates, powers etc..
- Every STRIKE3 monitoring site (no matter how well protected, how remote) has detected jammers
- There are very few examples of high power, long duration events
- It is very difficult to identify the cause of unintentional RF interferences

FOI

Sammanfattning

- Most RF interference events are low power (narrow/wide band)
  - Zero impact on GNSS receiver operations
- Most jammer waveforms are “chirp”
  - STRIKE3 has also detected emergence of advanced jammer waveforms
- Jamming events have very different power levels
- Jammer waveforms “appear” to have “uniqueness “within their signatures
  - Potentially due to use of low cost, low quality electronic components
- Jammers can result in:
  - No impact on positional information
  - Degraded performance of positioning
  - Total loss of positional information
- Modern GNSS receivers are effective at removing unintentional narrow band interferences
- Modern GNSS professional antennas offer some protection against interference

FOI

Fortsättning

- Swedavia Polisen/Tullverket
- Två interna ML kompetenssatsningar
- MSB studie?
  - Nationellt monitorering av GNSS
- GALACTIC (inskickat 5/3) ?
  - GNSS BigData, molnlagring, applikationer som använder rådata, detektion och lokalisering
  - 2.2 MEuro (FOI 4 Msek)
- Övriga?

RF Interferences to GNSS detected from 1/2/2016 – 11/12/2018

Number of RF interferences that are GNSS jammers

FOI