Initial Findings from the STRIKE3 GNSS Interference Monitoring Network

Mark Dumville
General Manager, NSL

Space Based PNT Advisory Board
21st Meeting, 16-17 May 2018, Baltimore, US

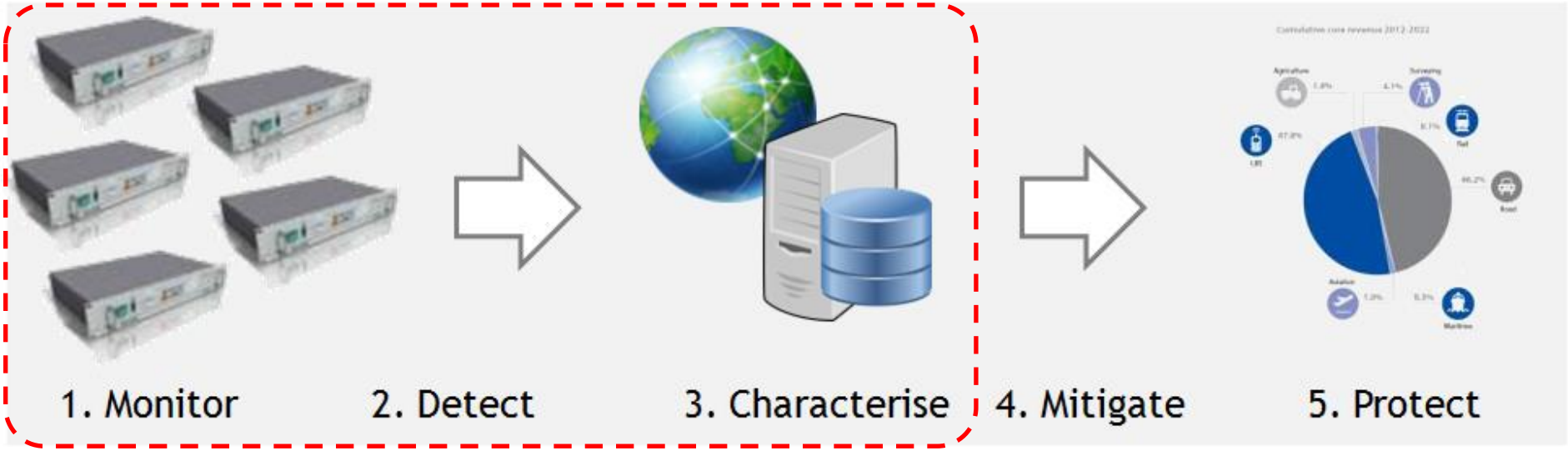
STRIKE3 is a project to protect GNSS…

- Standardisation of GNSS Threat reporting and Receiver testing through International Knowledge Exchange, Experimentation and Exploitation **[STRIKE3]**

- Project funded by European GNSS Agency (GSA) under the European Commission's H2020 Framework Programme

- Start date = 1 February 2016
- Duration = 3 years

STRIKE3 Project Rationale



- STRIKE3 will deploy and operate an international GNSS interference monitoring network (with support from partners)

- STRIKE3 will use the data from the network to ensure that there is:
  - a standard for GNSS threat reporting and analysis
  - a standard for assessing the performance of GNSS receivers and applications under threat.

STRIKE3 International Monitoring Network

At a range of infrastructures

- Major City Centres
- City-ring roads
- National timing labs
- Motorways/Road network
- Airports
- GNSS infrastructures
- Power stations
- Railway
- EU Borders
- Ports

At a range of locations

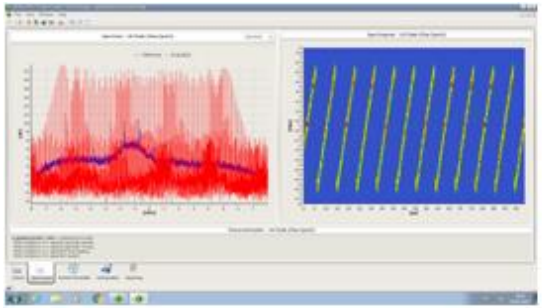
- United Kingdom
- Sweden
- Finland
- Germany
- France
- Poland
- Czech Republic
- Spain
- Slovakia
- Slovenia
- Netherlands
- Belgium
- Croatia
- Latvia
- India
- Vietnam
- Thailand
- Malaysia
- New Zealand
- Canada
- Japan (pending)
- US (exploring)
- Singapore (exploring)

Involving a range of entities:

- Government agencies
- Frequency regulators
- Road operators
- Tolling operators
- Airport operators
- Air Navigation Service Providers
- Power grids
- Research

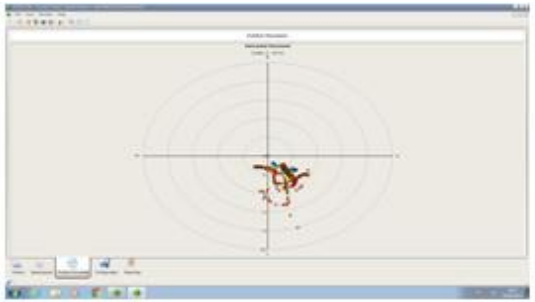
30+ monitoring sites

STRIKE3 Analysis Tool

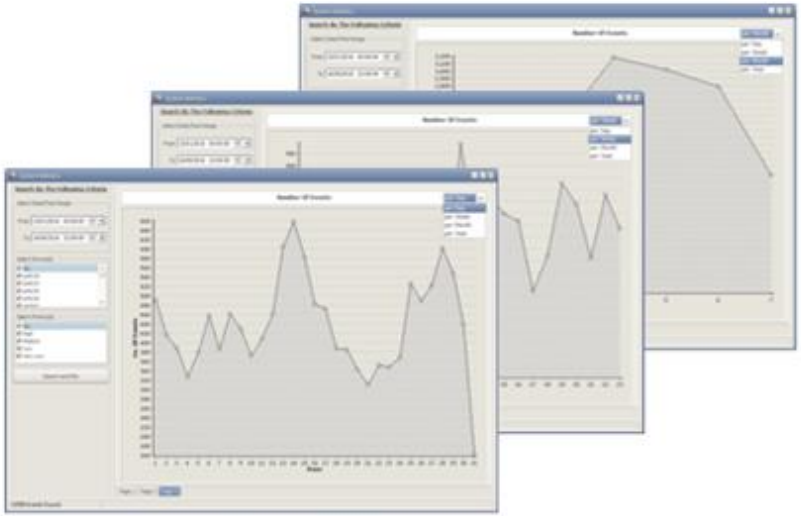


1. Spectrum/Spectrogram

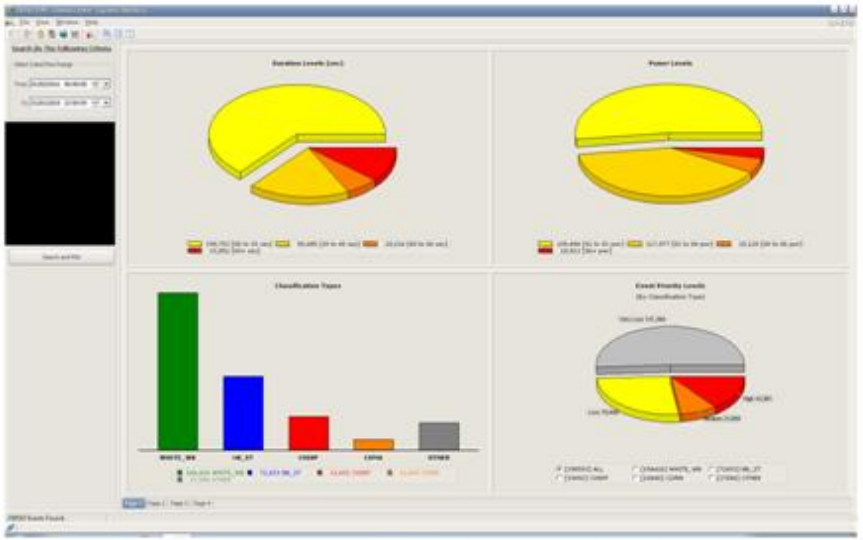
2. Event power profile and impact on number of Satellites



3. Impact on Positioning Accuracy



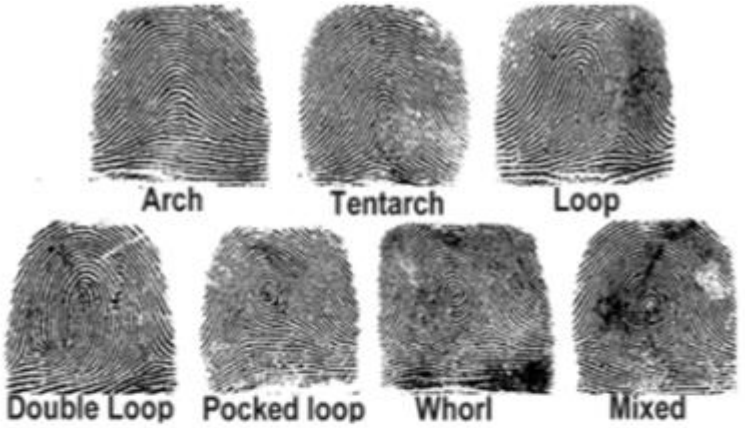
4. Trends statistics per site/group/all

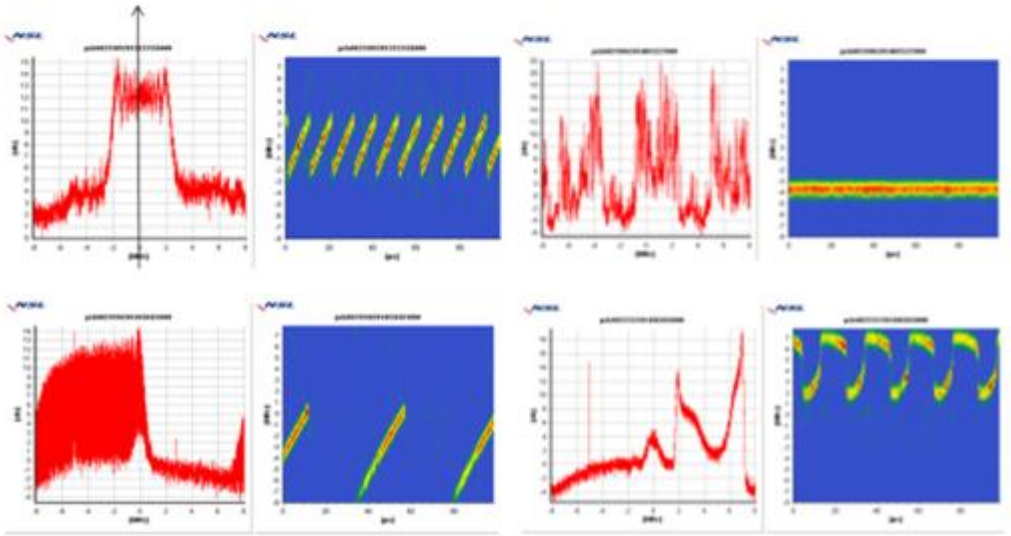


5. Summary statistics per site/group/all

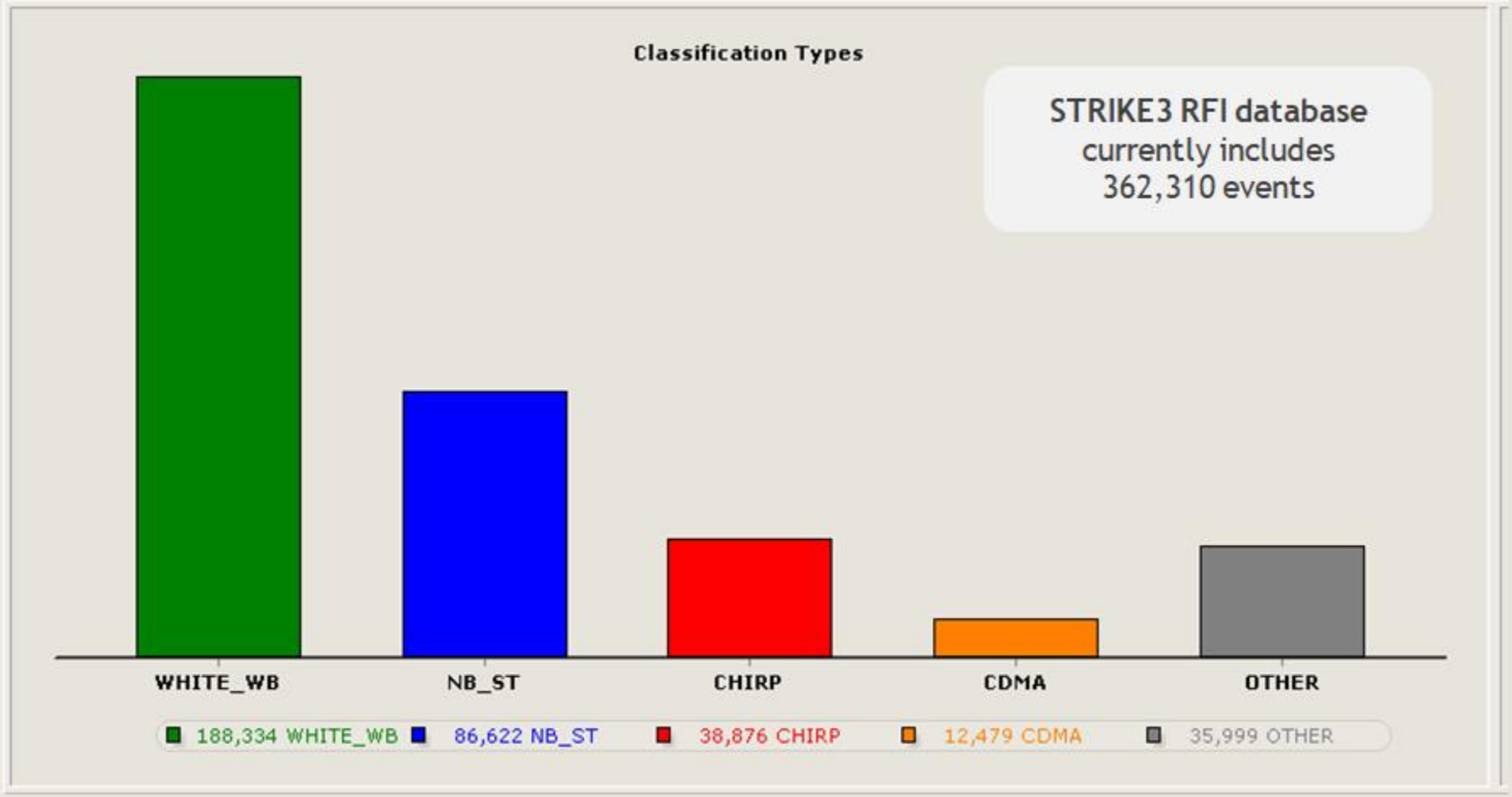
STRIKE3 Fingerprint characterisation

1. Size, pressure, patterns
2. Identify distinguishing features
3. Classify the signature
4. Identify different “families”
5. Identify new “families”
6. Preserve the evidence
   - Create a catalogue
   - Reference for future events
   - Automatic pattern recognition

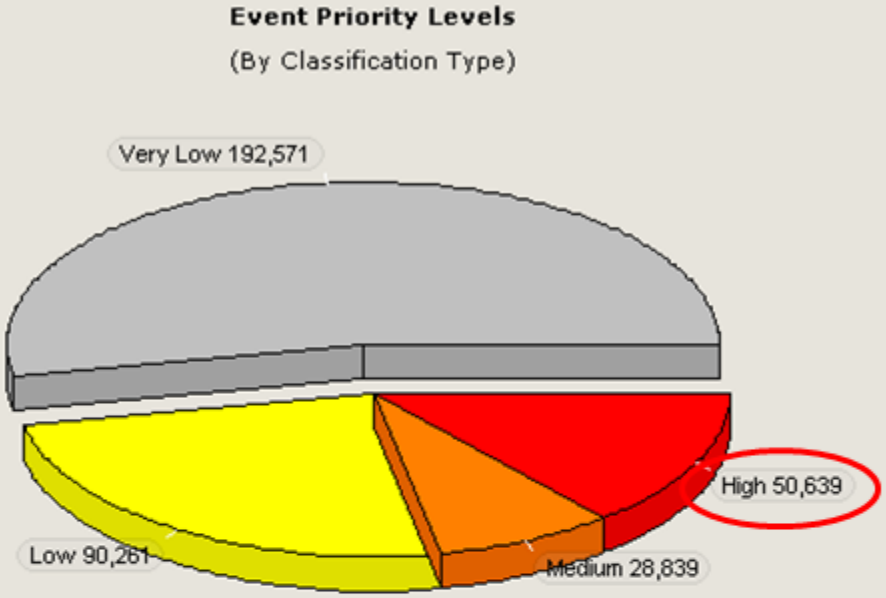




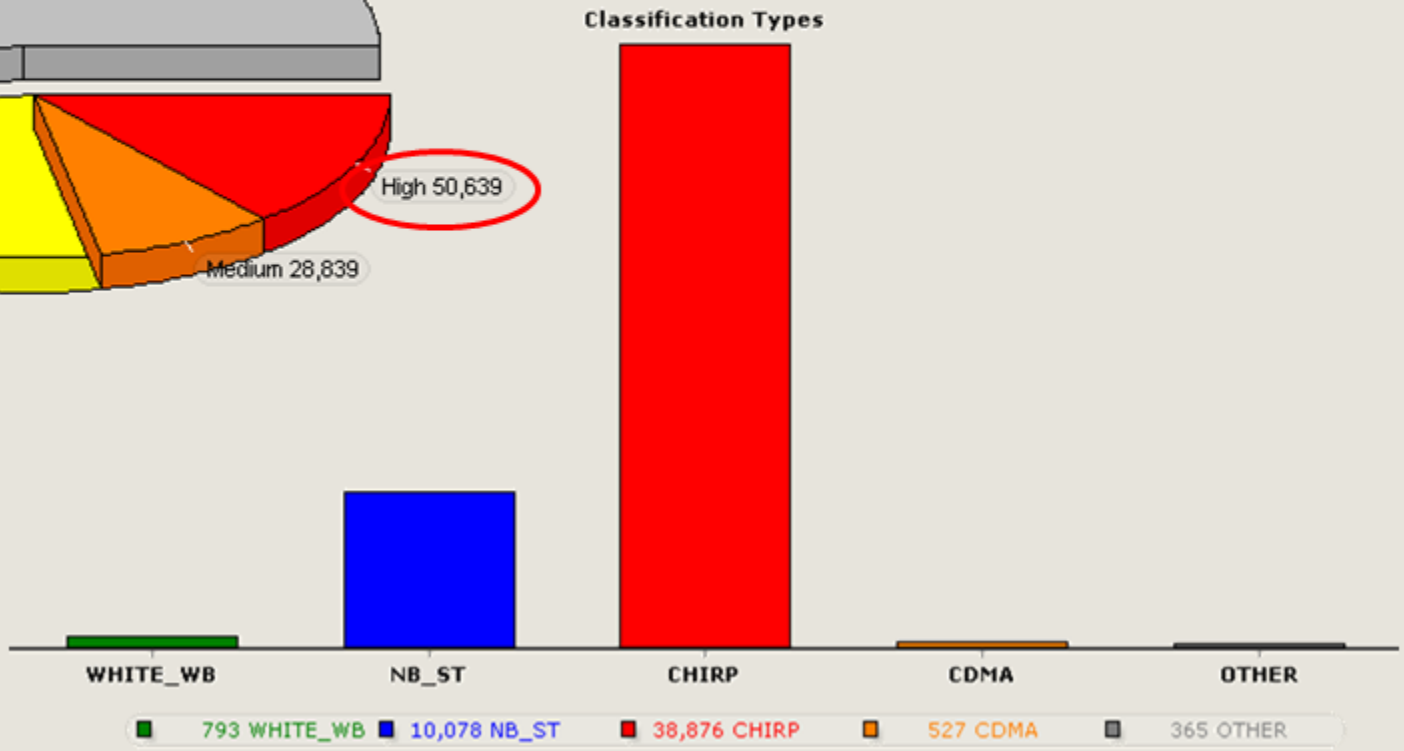
STRIKE3 “Database” [1/2/2016 – 30/04/2018]



STRIKE3 Denial Events [1/2/2016 – 30/04/2018]

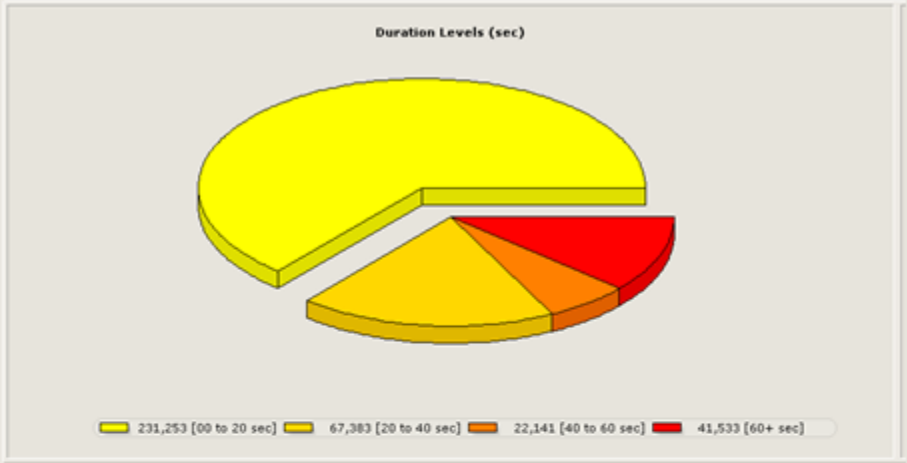


- 50,000 GNSS denial events:
  - 39,000 jammer events
  - 10,000 NB/single tone
  - 1,000 noise+CDMA+other



STRIKE3 “Durations” [1/2/2016 – 30/04/2018]

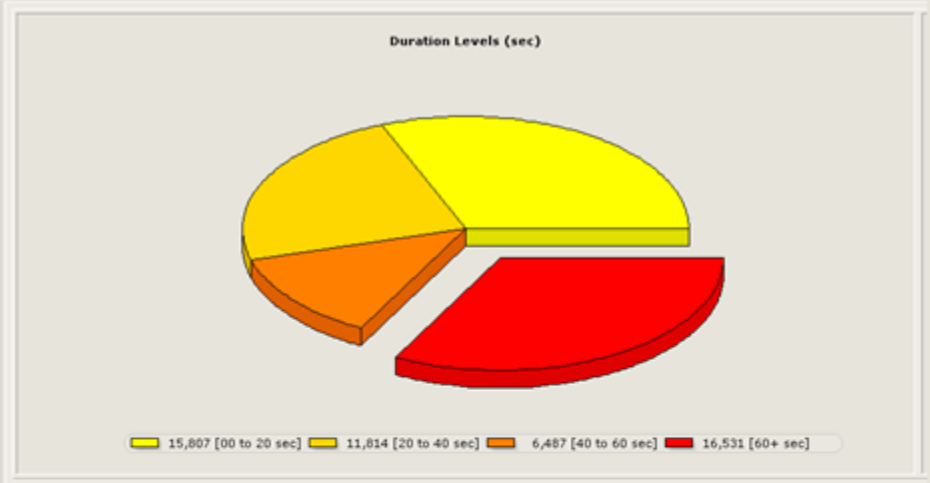
STRIKE3 database (362,000)



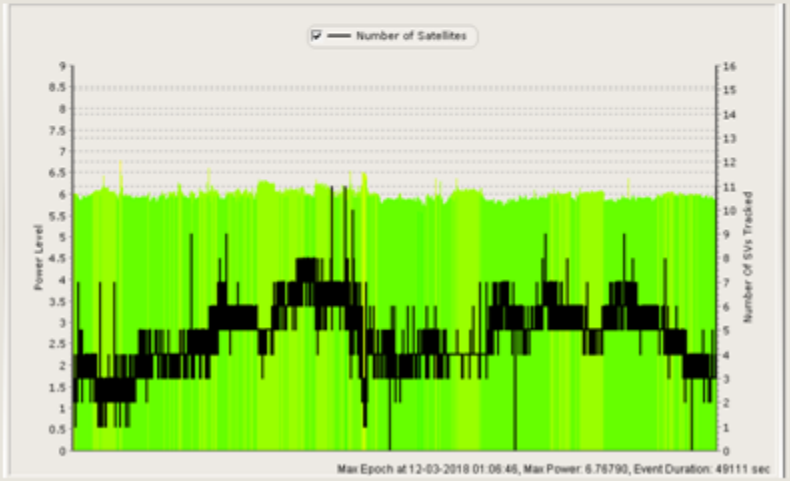
Most events are very short duration
11% of events are greater than 60secs

- 5840 events > 5 mins
- 972 events > 30mins
- 545 events > 60mins
- 5 events > 1 day
- Longest event = 5 days

STRIKE3 High Priority events (50,000)

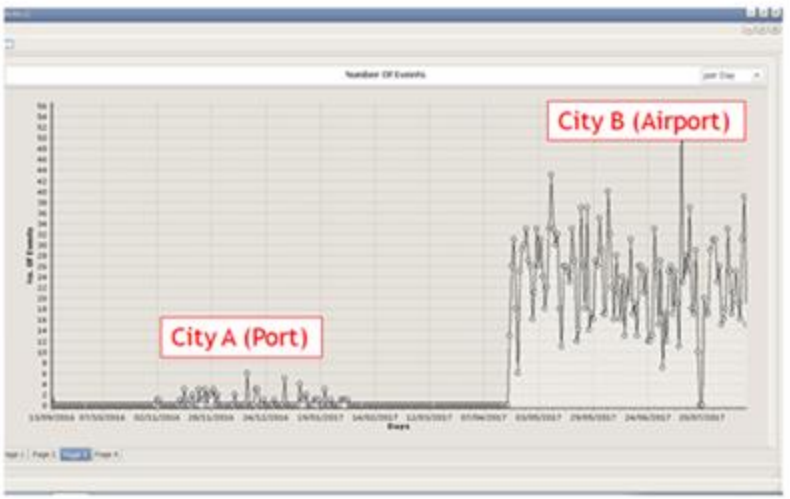


30% of events are greater than 60secs

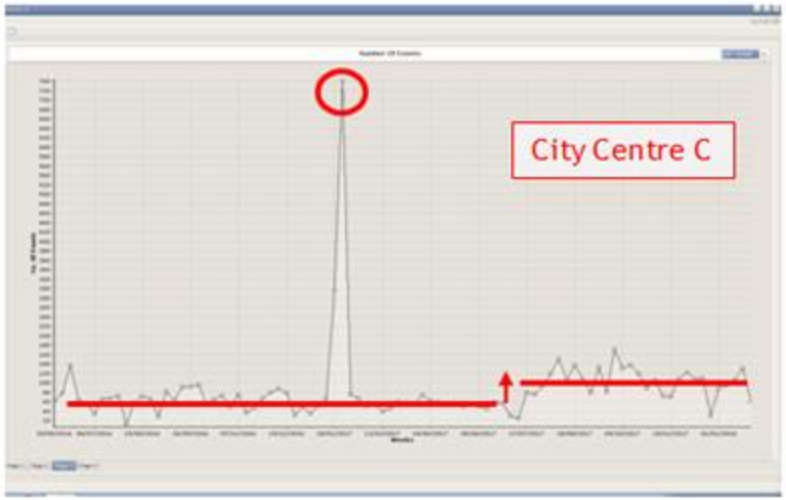


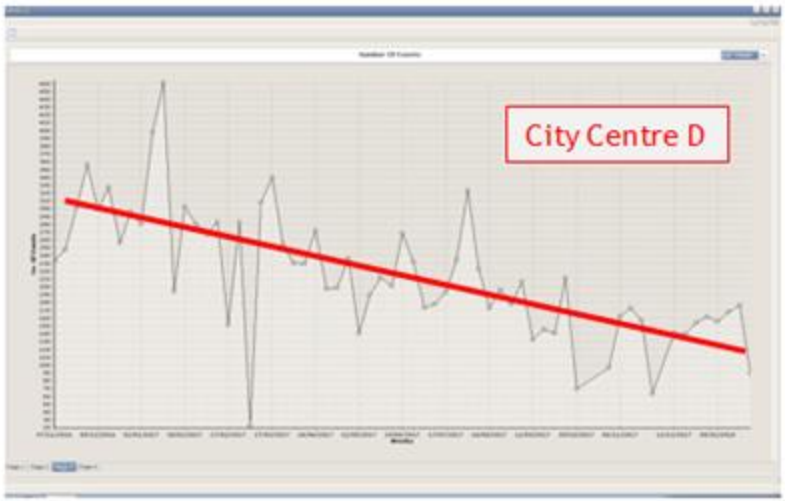
STRIKE3 Trend Analysis

- Trends per site
- Trends per infrastructure
- Trends per week/month/year
- Trends per grouping
- Trends per event classification
- Overall trends within the database
- *(Trends per GNSS, per frequency)*



Same DETECTOR, two different locations





Trends at two "city centre" sites

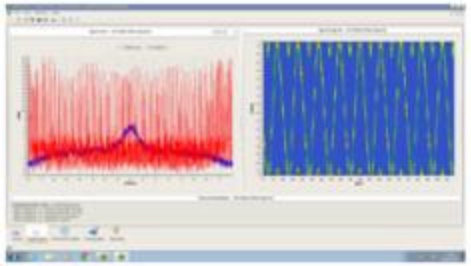
STRIKE3 Site Comparisons (Airports)

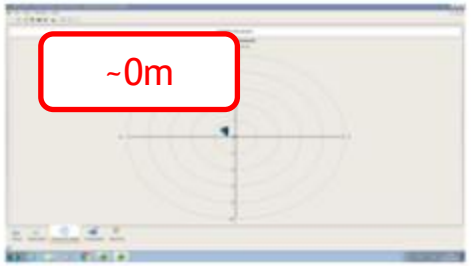
- Results from 8 Airport installations
- Most are “national” airports. Most are air-side installations.
- 30 days data (may not be the same 30 days)

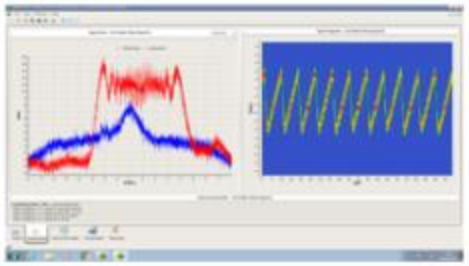
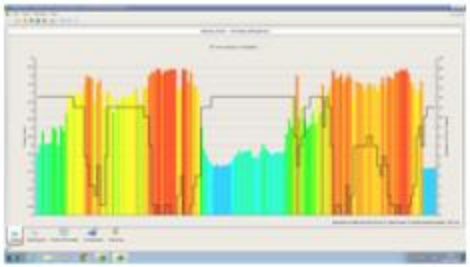
	RFI events	Jammers	Jammer/events ratio	Duration > 60secs	GNSS denial	Denial/events ratio
National Airport	8716	95	1%	282	362	4%
National Airport	759	27	4%	200	211	28%
National Airport	2764	595	22%	395	753	27%
Regional Airport	556	31	6%	6	95	17%
National Airport	904	168	19%	158	182	20%
National Airport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

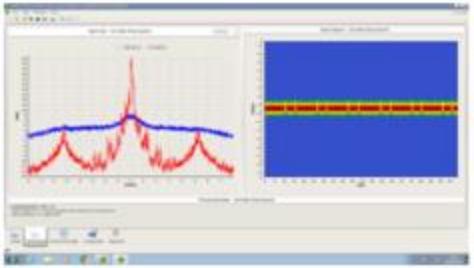
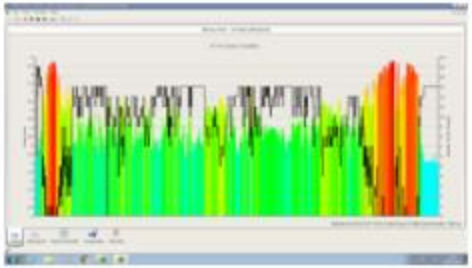
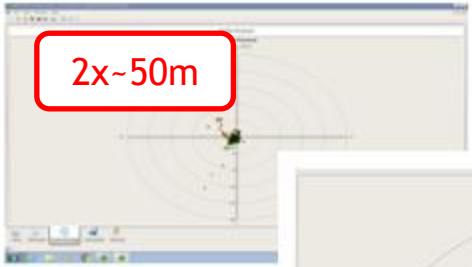
- Helps to diagnose issues with unintentional interference & jamming
- Helps to compare with other sites

STRIKE3 Impact Assessments

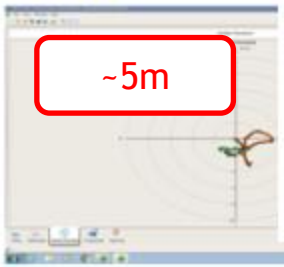


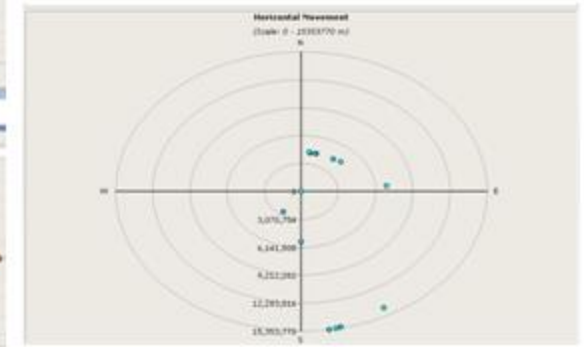


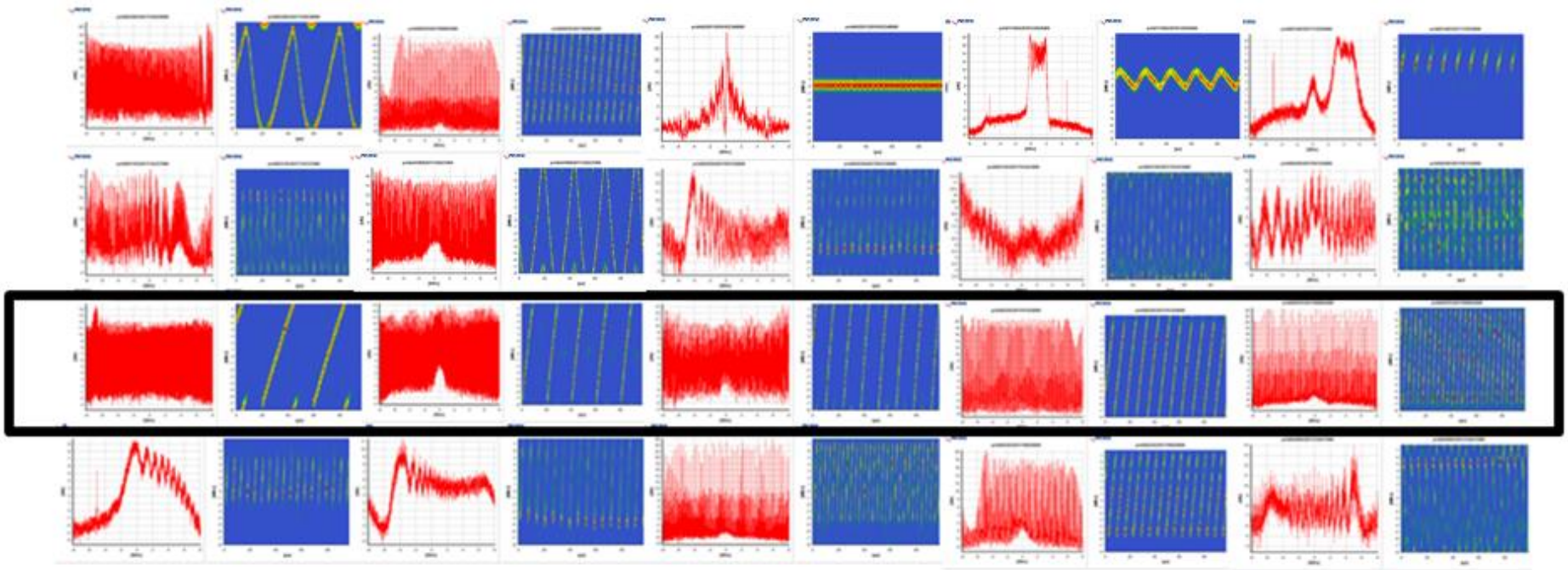




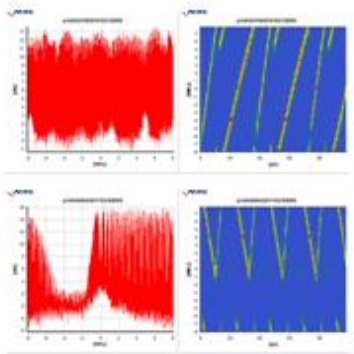


m's to km's

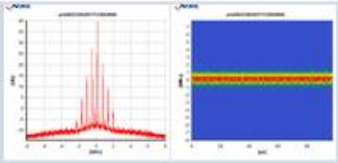
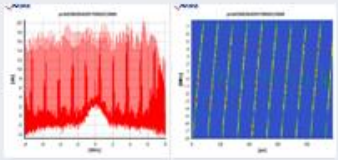
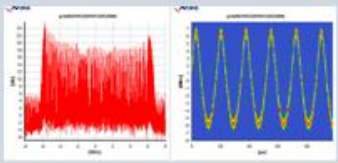
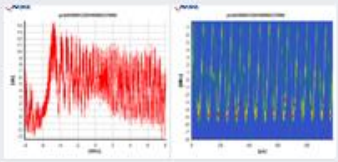
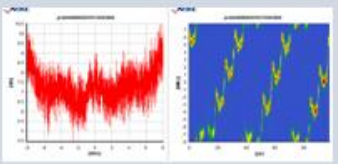
STRIKE3Jammer waveforms



- **There are lots of jammer waveforms, characterised by:**
  - Bandwidths, power, centre frequency, signal(s)
  - Additional parameters: sweep rate, direction, return

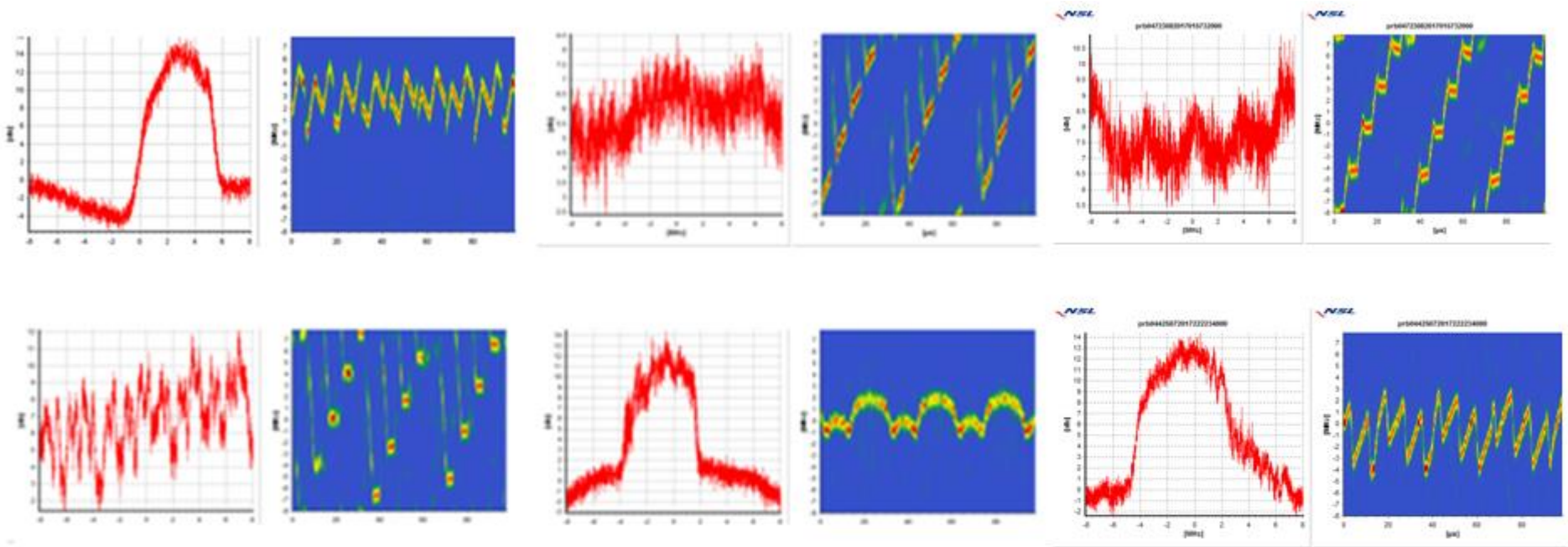


STRIKE3 Threat Testing waveforms

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).

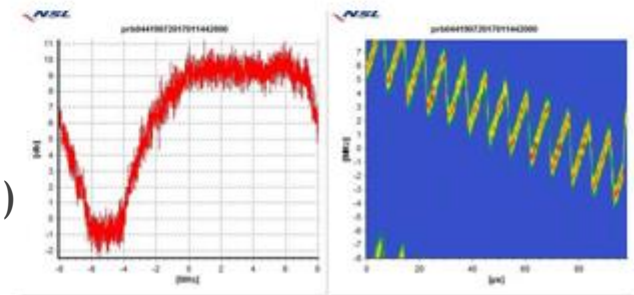
GNSS receiver industry should focus on mitigations for these popular waveforms

STRIKE3 Advanced (jammer) waveforms

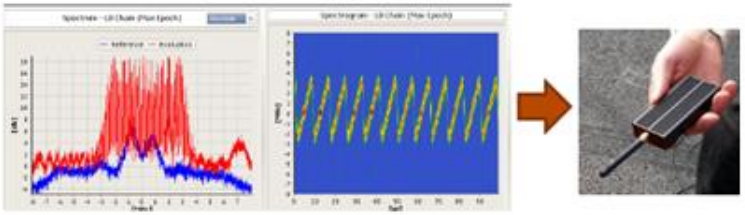


Simple Rules to support validation

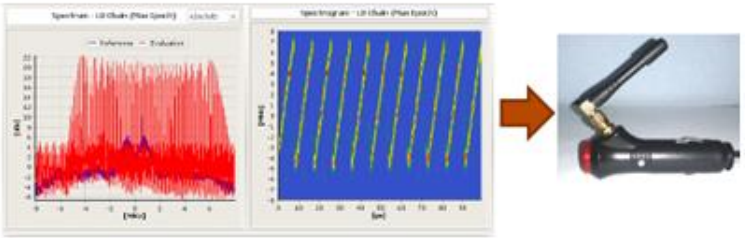
- It has a structure (it is deliberate, purposeful)
- It is mobile (exhibits same power profile as a jammer)
- It is seen multiple times (avoids being a one-off rogue “signal”)
- It is seen multiple sites (demonstrates a distributed product)



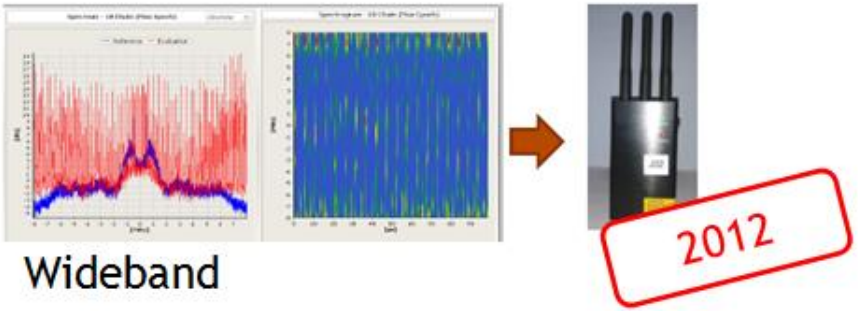
STRIKE3 shows Jammer industry is evolving...



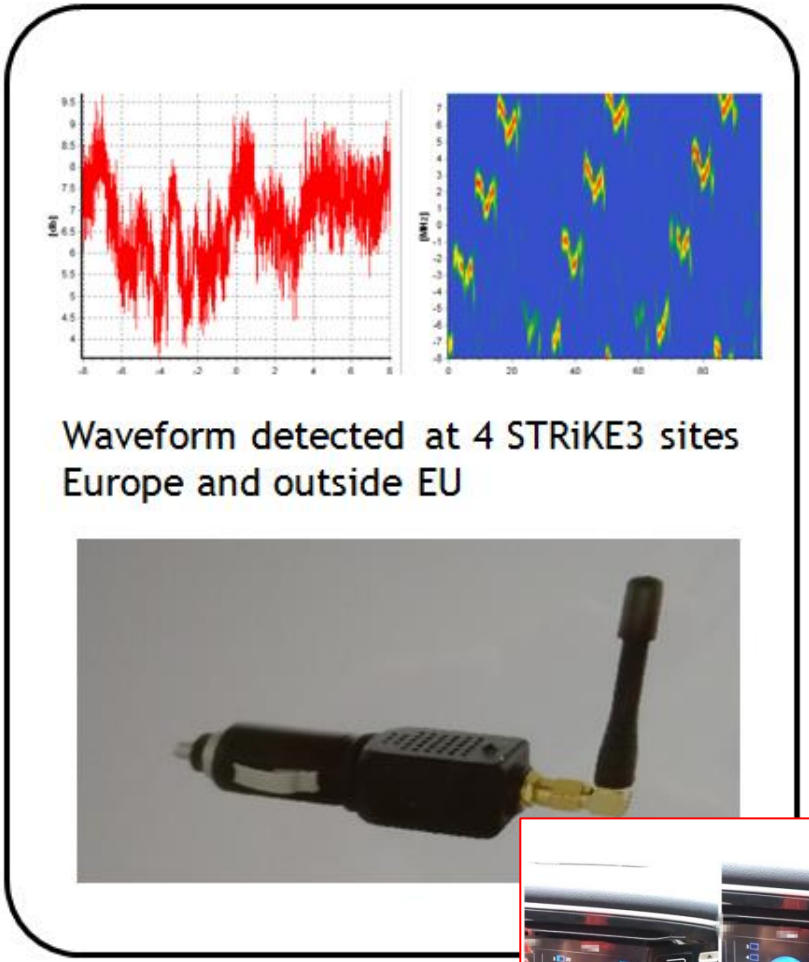
5Mhz bandwidth, 1575Mhz centred



8Mhz bandwidth, drifting centre



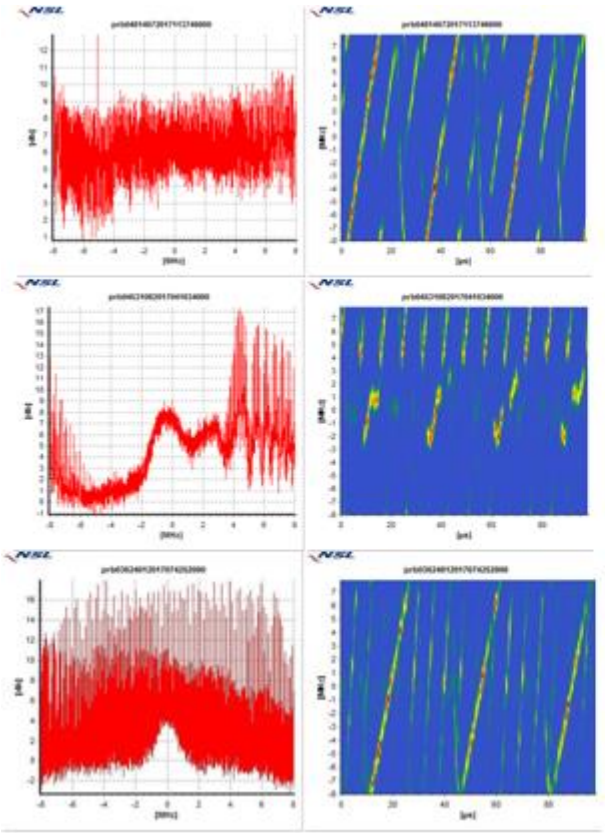
Wideband

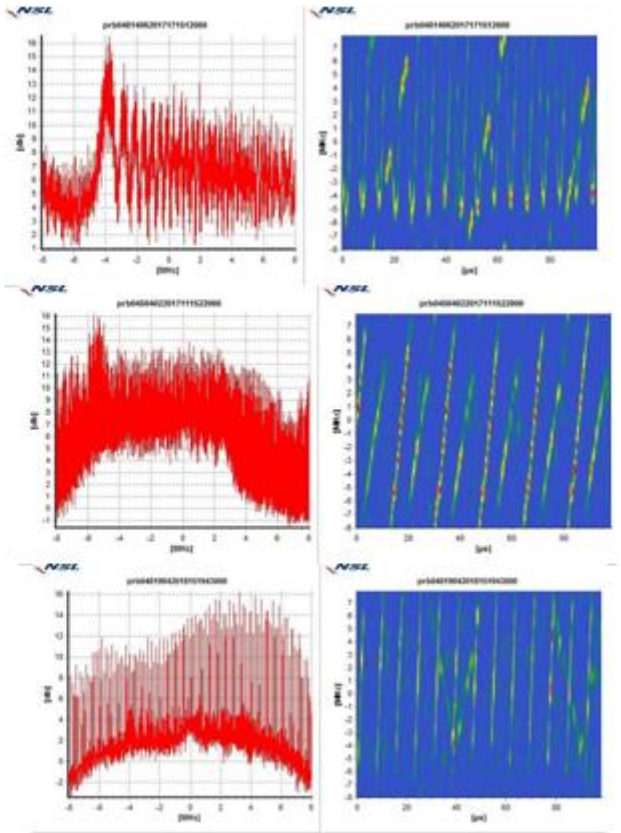


Waveform detected at 4 STRiKE3 sites Europe and outside EU

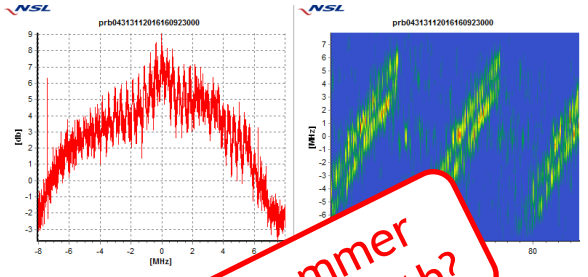
USB L1/L2 jammer

What are the chances? Same place, same time...



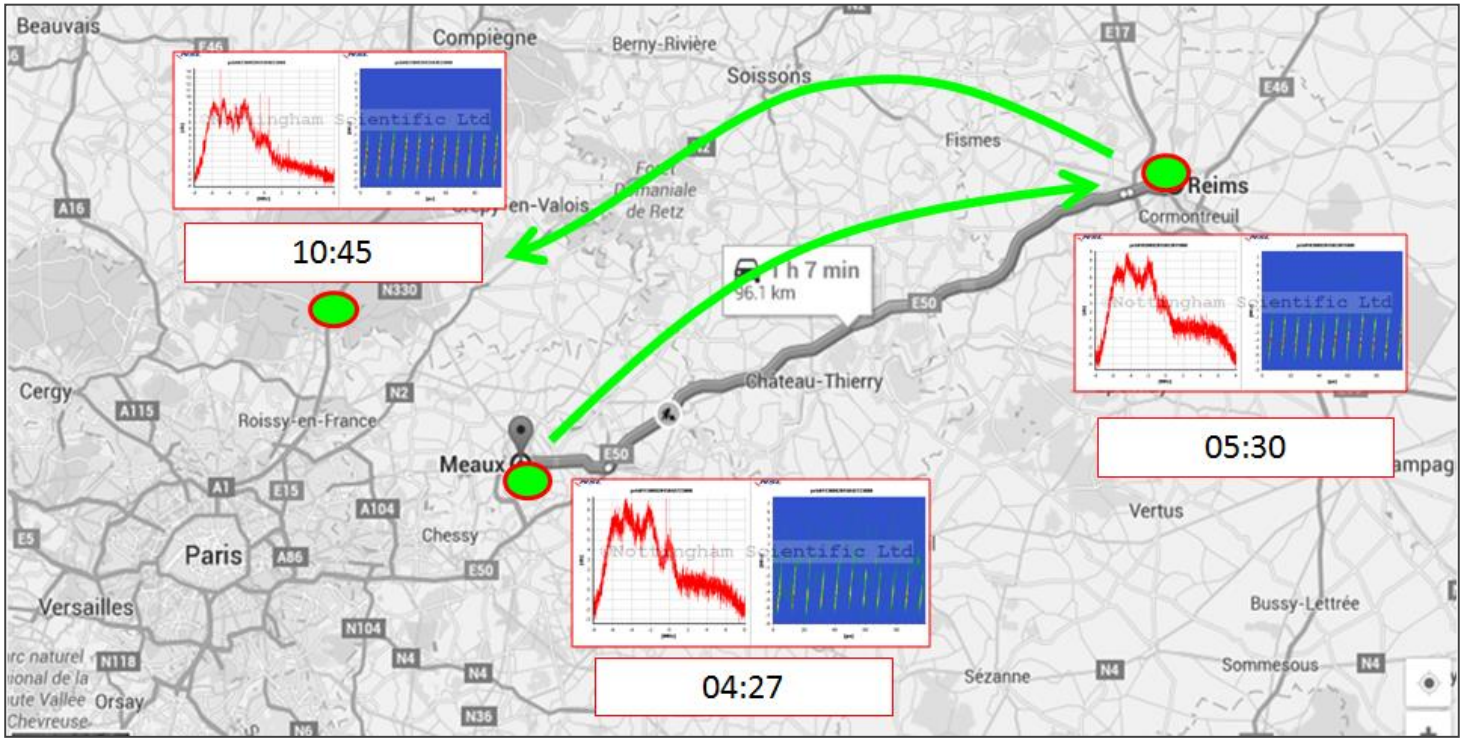


- Dual signal jammer?
- One vehicle, two jammers?
- Two vehicles, one jammer in each?
- Jammer in truck, jammer in trailer?

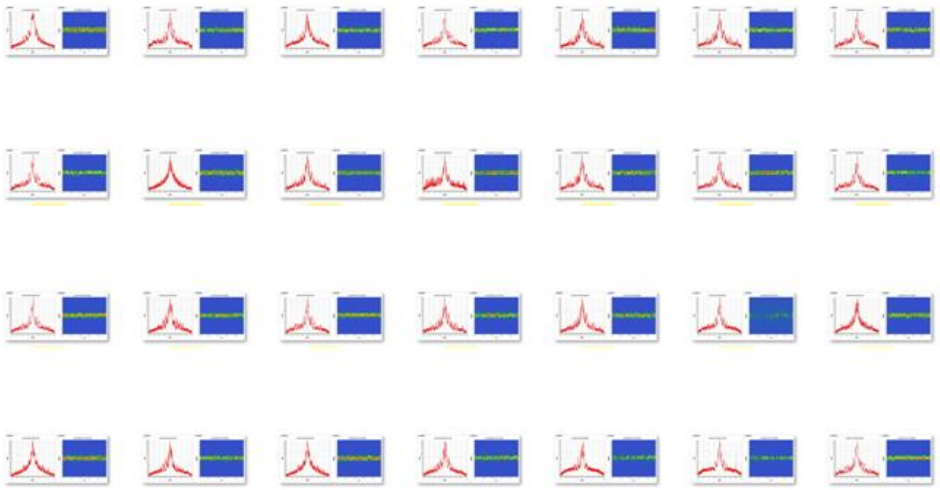


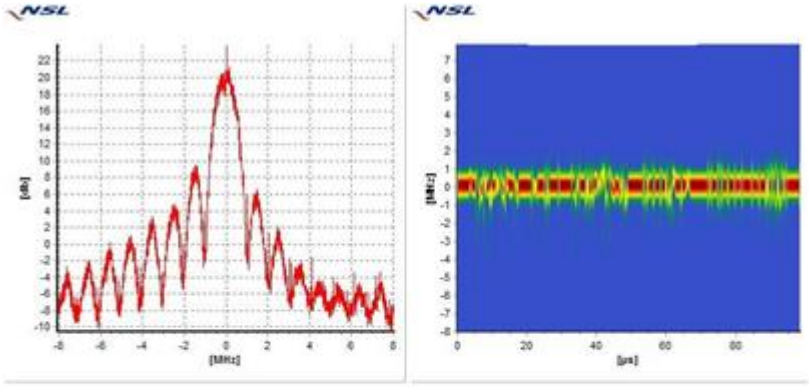
STRIKE3 demonstrates the value of characterisation...

1. Distinguish between “unintentional” and “deliberate” threats
   - Fingerprinting eliminates false “jammer” detections
   - Fingerprinting ensures correct statistics
2. Distinguish between different types of jammer (basic >> advanced >> exotic)
3. Identify repeat threat signatures (to assess the scale of the problem)
4. Enables you to “track a jammer” across/within a monitoring network



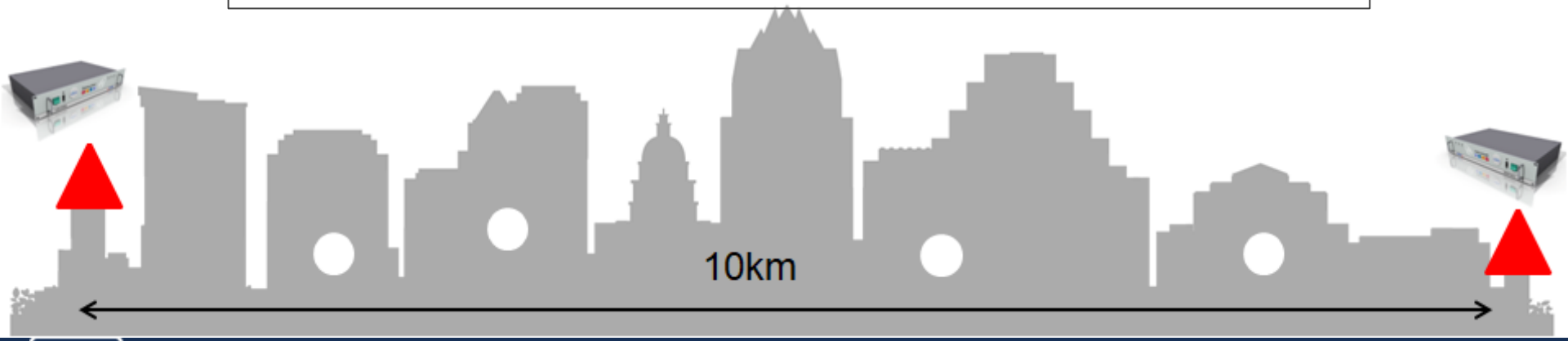
The last unknown within STRIKE3...





- Number of events = 4576
- Longest duration = 27504secs
- High power (but from a distance)
- Unable to identify cause

May 2018: Major Capital City. Two STRIKE3 sites, separated by 10km. Same waveform detected at same times



STRIKE3 Draft Standards

1. Standards for Threat Monitoring and Reporting
2. Standards for Receiver testing against threats


D4.1: Draft standards for threat monitoring and reporting

Ref: STRIKE3_D41_RepStandards Issue: 1.1_public Date: 20.03.17

STANDARDISATION OF GNSS THREAT REPORTING AND RECEIVER TESTING THROUGH INTERNATIONAL KNOWLEDGE EXCHANGE, EXPERIMENTATION AND EXPLOITATION

STRIKE3

D4.1: DRAFT STANDARDS FOR THREAT MONITORING AND REPORTING

Prepared by:	M Pattinson (NSL), D Fryganiotis (NSL), P Ellardsson (FOI)	20/03/17
Checked by:	M Dumville (NSL)	20/03/17
Authorised by:	M Dumville (NSL)	20/03/17

Document Classification: Public Pages: 25

Document Classification: Public Page 1 of 25


D4.2: Draft standards for receiver testing against threats

Ref:STRIKE3_D42_TestStandards Issue: 1.0 Date: 03.02.17

STANDARDISATION OF GNSS THREAT REPORTING AND RECEIVER TESTING THROUGH INTERNATIONAL KNOWLEDGE EXCHANGE, EXPERIMENTATION AND EXPLOITATION

STRIKE3

D4.2: DRAFT STANDARDS FOR RECEIVER TESTING AGAINST THREATS

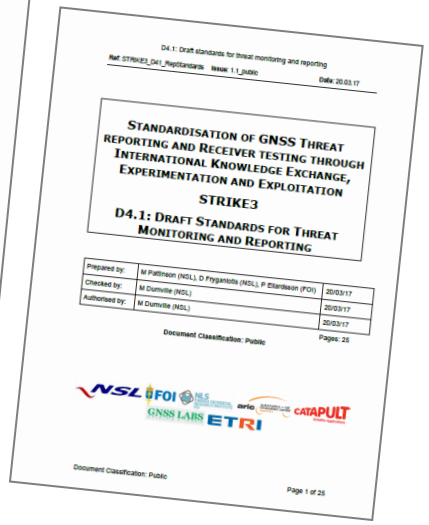
Prepared by:	Steve Hill, Satellite Applications Catapult Ltd Ghassan Ameer, Satellite Applications Catapult Ltd Sanguk Lee, ETRI Venkatesh Manikundalam, GNSS Labs	03.02.17
Checked by:	M Pattinson (NSL)	03.02.17
Authorised by:	M Dumville (NSL)	03.02.17

Document Classification: Public Pages: 50

Document Classification: Public Page 1 of 50

Available from: www.gnss-strike3.eu

What next for STRIKE3?



- **Deployment of a national STRIKE network**
  - Multi-GNSS, multi-frequency
  - At sites of critical national infrastructure
- **Validate the STRIKE3 reporting standard**
  - System of systems Threat database
- **Integration of crowd-sourced GNSS RINEX data to:**
  - Identify GNSS interference hotspots
  - Understand the impact of wide area (high power) events on GNSS receivers
- **Testing GNSS receivers against the "STRIKE3 threat database"**
  - Support the development of new interference mitigation techniques

STRIKE3 live-sky demonstration and project close-out workshop in late 2018

Thank you for the opportunity to present and to participate

Mark.dumville@nsl.eu.com
General Manager, NSL

Space Based PNT Advisory Board
21st Meeting, 16-17 May 2018, Baltimore, US