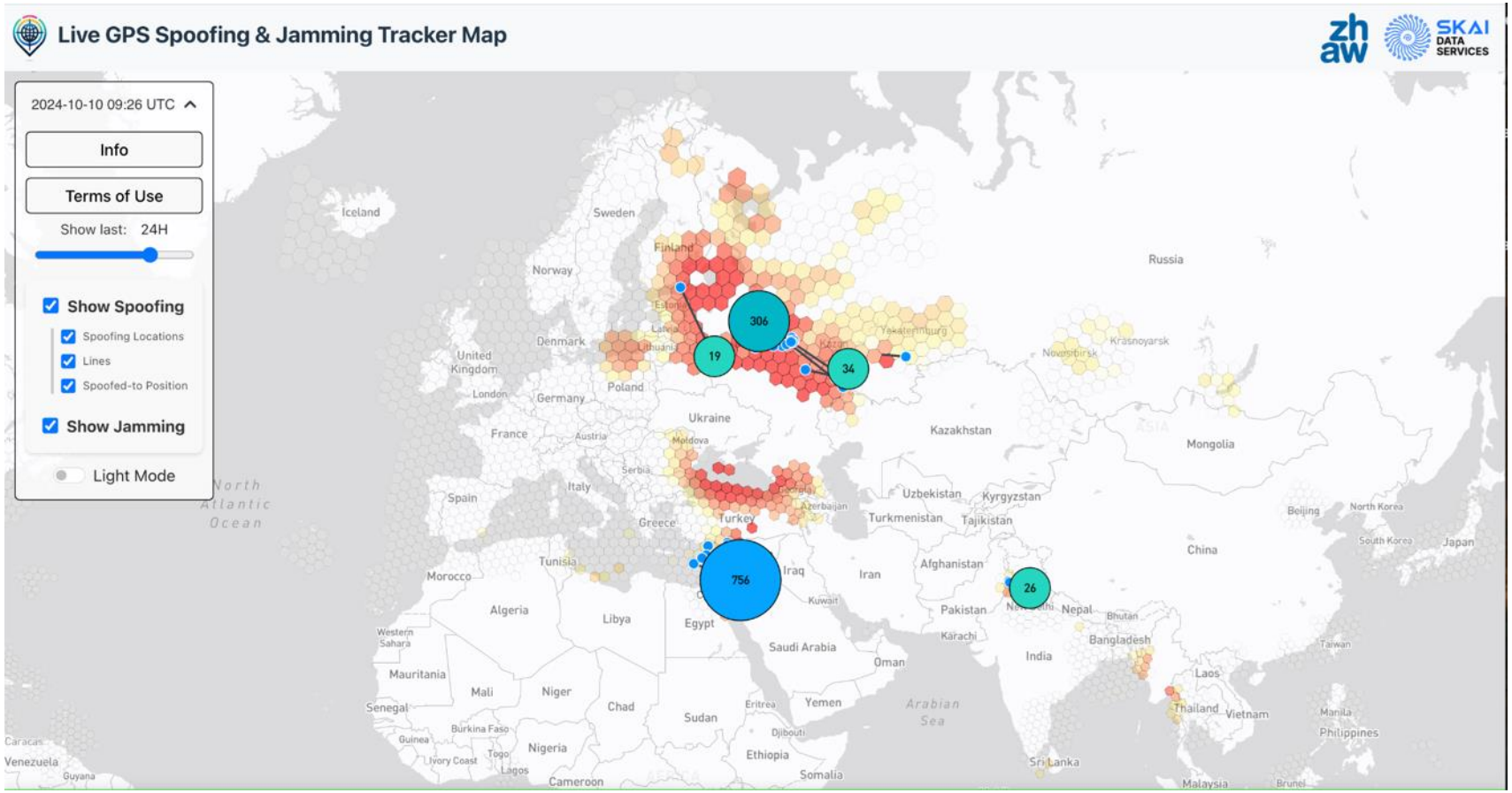
Resilient PNT Best Practice Guidelines

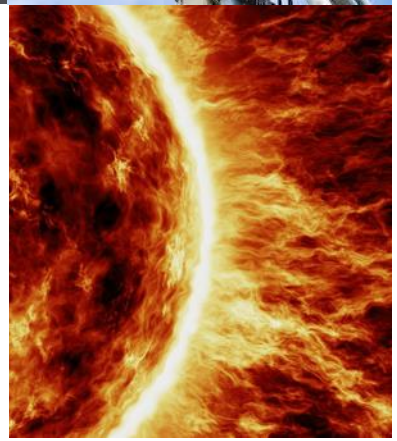
Dr Ramsey Faragher

Director and CEO, Royal Institute of Navigation

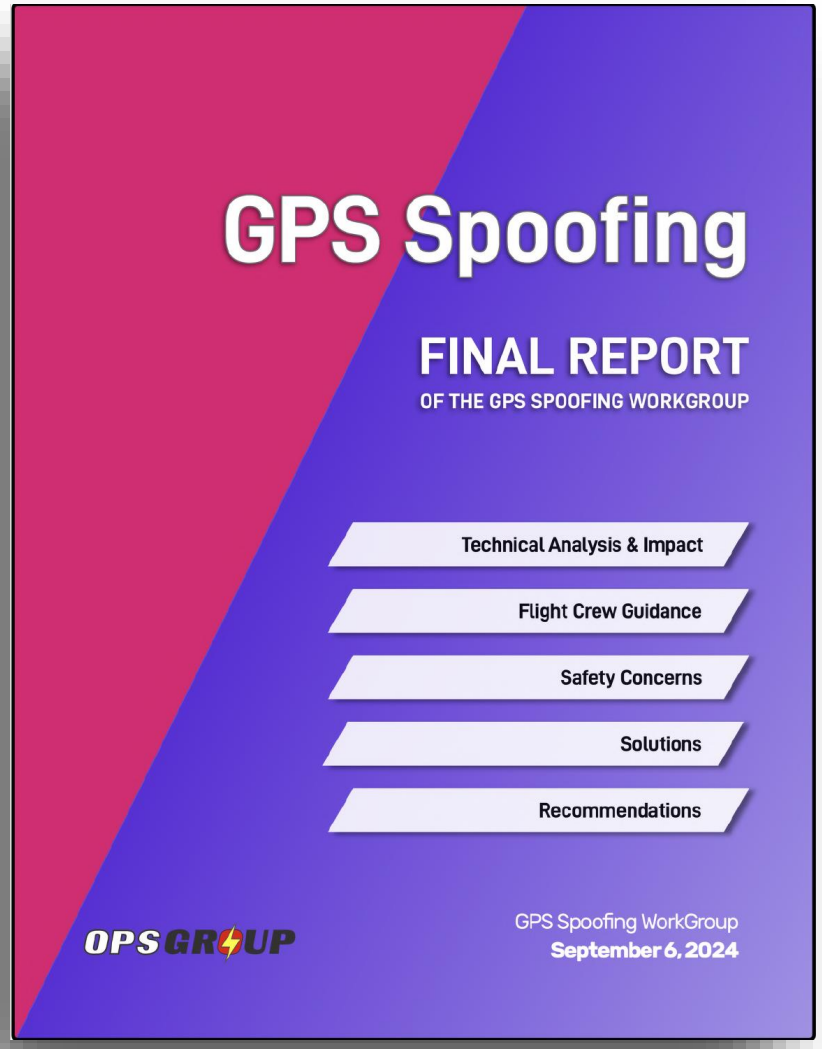
Fellow, Queens' College University of Cambridge

The need for Resilient PNT





Civil aviation spoofing - a wake up call



- Over 1500 flights impacted by interference per day
- During/after interference 20-30 systems can fail or misbehave onboard
- ~8% of the time hardware needs to be physically replaced
- Mitigation procedures involve disabling systems in flight using the circuit breakers
- The human pilots are the key to the current mitigations working - automated systems fail
- If this is happening to airliners what could happen to nuclear power stations? Water purification plants? Telecommunications? Banking? ...

The Royal Institute of Navigation (RIN) have launched the world's first set of best practice principles and checklist for resilient Positioning, Navigation and Timing (PNT).

The new guidance and checklist provide clear and actionable advice on how to assess and mitigate PNT risks, develop robust contingency plans, and invest in innovative PNT technologies. The principles and checklist can be found on the Royal Institute of Navigation's website.

The Department for Science, Innovation and Technology (DSIT) worked with the RIN on developing the principles and guidance including part funding the work.

Royal Institute Of Navigation

RESILIENT PNT RESOURCES PORTAL

BEST PRACTICES ONE PAGER

PNT EXPLAINER

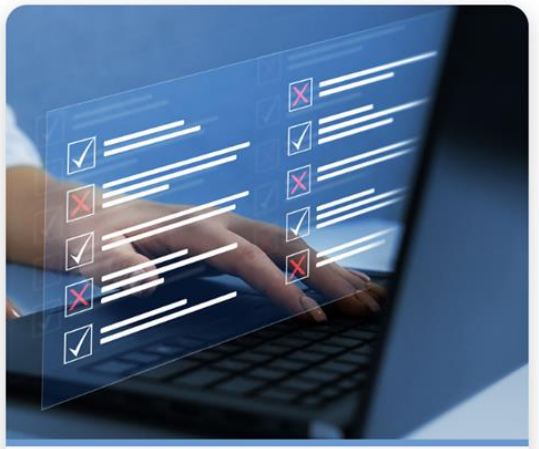
Positioning, navigation and timing (PNT) is widely used in our daily lives. Simply put, modern life is reliant on PNT working. But PNT is vulnerable. Learn more here.

MORE

RESILIENT PNT BEST PRACTICES

Our straightforward "Prepare > Act > Recover" best practices approach will improve your preparedness. Read and download here.

MORE



PNT RESILIENCE CHECKLIST

Use our prctical 10 point checklist now to identify what you've got covered and where you may need to be better prepared.

MORE

PRACTICAL GUIDANCE

There are practical steps you can take to improve resilience and preparedness. Learn more here.

MORE

PNT TRAINING RESOURCES

We have a range of training and CPD resources available to improve knowledge and understanding of resilient PNT.

MORE

CASE STUDIES COMING SOON...

More information and resources coming soon.

MORE

https://rin.org.uk/Resilient_PNT

Programme aims

- Provide operational guidance for non-technical decision makers
- Provide tools that can enable CNI operators and suppliers to “score” and visualise their resilience

- Encourage new behaviours - e.g. an annual “fire drill”
- Encourage a continuous-improvement mentality to Resilient PNT

- Resilient PNT is a mindset, not an expensive piece of hardware

UK’s Critical National Infrastructure

Chemicals
Civil Nuclear
Communications
Defence
Emergency Services
Energy
Finance
Food
Government
Health
Space
Transport
Water

Programme spanning 18 months

March 2024

Phase 1

Resilient PNT Principles

November 2024

Phase 2

Resilient PNT Best Practices Guidance

Cross-domain audience
includes C-suite

March 2025

Phase 3

Sector specific Guidance

CNI #1

CNI #2

…

CNI #13

Sector specific
Systems integrators
Technical audience

October 2025

Key Principles for Resilient PNT

Key Principles for Resilient PNT

PREPARE FOR PNT DISRUPTIONS

1. Include PNT resilience in existing governance, cyber-risk, and business continuity frameworks.
2. Test system responses to understand effects of PNT disruptions on system behaviour.
3. Build a mitigation strategy to improve resilience and preserve safety, security and economic performance.

ACT WHEN PNT DISRUPTIONS OCCUR

1. Detect disruption events as soon as possible after they occur.
2. Take planned steps to preserve essential levels of safety, security, and economic wellbeing.
3. Monitor, measure, and record the impact of disruptions on system performance.

RECOVER FROM PNT DISRUPTIONS

1. Return to standard operations when safe and secure to do so.
2. Assess mitigation effectiveness and update response plans and continuity frameworks.
3. Share lessons learned when reporting incidents and their associated impacts.

Key Principles for Resilient PNT

PREPARE FOR PNT DISRUPTIONS

1. Include PNT resilience in existing governance, cyber-risk, and business continuity frameworks.
2. Test system responses to understand effects of PNT disruptions on system behaviour.
3. Build a mitigation strategy to improve resilience and preserve safety, security and economic performance.

Key Principles for Resilient PNT

PREPARE FOR PNT DISRUPTIONS

1. Include PNT resilience in existing governance, cyber-risk, and business continuity frameworks.
2. Test system responses to understand effects of PNT disruptions on system behaviour.
3. Build a mitigation strategy to improve resilience and preserve safety, security and economic performance.

Key Principles for Resilient PNT

ACT WHEN PNT DISRUPTIONS OCCUR

1. Detect disruption events as soon as possible after they occur.
2. Take planned steps to preserve essential levels of safety, security, and economic wellbeing.
3. Monitor, measure, and record the impact of disruptions on system performance.

Key Principles for Resilient PNT

ACT WHEN PNT DISRUPTIONS OCCUR

1. Detect disruption events as soon as possible after they occur.
2. Take planned steps to preserve essential levels of safety, security, and economic wellbeing.
3. Monitor, measure, and record the impact of disruptions on system performance.

Key Principles for Resilient PNT

RECOVER FROM PNT DISRUPTIONS

1. Return to standard operations when safe and secure to do so.
2. Assess mitigation effectiveness and update response plans and continuity frameworks.
3. Share lessons learned when reporting incidents and their associated impacts.

Key Principles for Resilient PNT

RECOVER FROM PNT DISRUPTIONS

1. Return to standard operations when safe and secure to do so.
2. Assess mitigation effectiveness and update response plans and continuity frameworks.
3. Share lessons learned when reporting incidents and their associated impacts.

GPS Spoofing

FINAL REPORT

OF THE GPS SPOOFING WORKGROUP

- Technical Analysis & Impact
- Flight Crew Guidance
- Safety Concerns
- Solutions
- Recommendations

OPSGROUP

GPS Spoofing WorkGroup
September 6, 2024

GPS SPOOFING GUIDANCE

FOLLOW OPERATOR AND OEM GUIDANCE FIRST

OPSGROUP
AUG 2024 / NO © / FREE TO RE-USE

PRE-FLIGHT

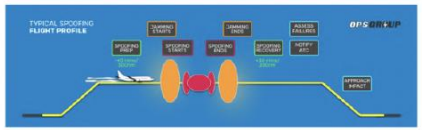
- **Pre-Flight Briefing** Spoofing area locations, intentions, ground-based navaids, likely system losses, indications of spoofing, contingencies/emergencies.
- **Spoofing Maps** - Review
- **GPWS** - Review likely impacts, action plan
- **IRS** Full alignment, manually if in spoofing area
- **Flight Planning** - File on navaid-based airways, review Cb activity (Wx Radar failure), avoid RNP approaches.
- **Sync watches, Check MEL** items, refresh technical understanding.

PRE-SPOOFING

- **Prepare** setup by 45 mins/300nm prior spoofing area
- **Re-Brief Plan** - actions, signs, systems loss
- **Monitor** - EPU/ANP, open sensor/POS REF page, anticipate jamming first, monitor clock.
- **Increase Vigilence** - Unusual system behavior, cross check to handheld GPS, alerting app, ATC reports
- **Set up aircraft systems** - Follow OEM/Opr guidance, de-select GPS to FMS, de-select IRS Hybrid, clock to INT, inhibit EGPWS Look-ahead mode, stow HUD.

IN SPOOFING

- **Aviate, navigate, communicate** - back to basics.
- **Note time** on personal watch, record on log
- **Check system settings** correct for spoof protection
- **Check GPS input** de-selected
- **Check IRS Hybrid mode** de-selected
- **Heading mode** if needed
- **Confirm Nav source** in FMS
- **Report to ATC**, request vectors if needed
- **Inhibit EGPWS** at cruise alt, if procedure allowed



JAMMING Indications

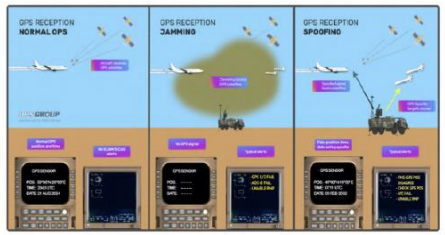
- GPS Failure message
- ADS-B Failure/Warning
- GPWS Terrain caution message
- SATCOM loss
- EGPWS Terrain fail
- Loss of SVS

SPOOFING Indications

- GPS position disagree message
- Rapid EPU/ANP increase
- Aircraft Clock time change
- Transponder fail
- Uncommanded autopilot turn
- Synthetic vision reversion
- Wind indicator illogical
- GPS posn on ND differs from FMS posn
- See full guidance text for complete list

RECOVERY

- **Be certain spoofing finished**
- **Check GPS sensor page** for correct time, date, GS, alt.
- **Assess** all systems for failures
- If allowed, carry out in-flight reset of MMR/GPS/GPWS
- Re-select GPS sensor input to FMS
- Advise ATC of remaining failures
- **Oceanic:** early message to OACC of RNP/CPDLC/ADS-C failures, anticipate lower crossing alt/reroute.
- **Appoach:** Avoid RNP approaches, advise ATC, brief intentions re. EGPWS false alerts, basic modes, possible ECAM/EICAS alerts, check alternates



PREPARE FOR PNT DISRUPTIONS

1. Include PNT resilience in existing governance, cyber-risk, and business continuity frameworks.
2. Test system responses to understand effects of PNT disruptions on system behaviour.
3. Build a mitigation strategy to improve resilience and preserve safety, security and economic performance.

ACT WHEN PNT DISRUPTIONS OCCUR

1. Detect disruption events as soon as possible after they occur.
2. Take planned steps to preserve essential levels of safety, security, and economic wellbeing.
3. Monitor, measure, and record the impact of disruptions on system performance.

RECOVER FROM PNT DISRUPTIONS

1. Return to standard operations when safe and secure to do so.
2. Assess mitigation effectiveness and update response plans and continuity frameworks.
3. Share lessons learned when reporting incidents and their associated impacts.

GPS SPOOFING GUIDANCE

FOLLOW OPERATOR AND OEM GUIDANCE FIRST

OPSGROUP

AUG 2024 / NO © / FREE TO RE-USE

PRE-FLIGHT

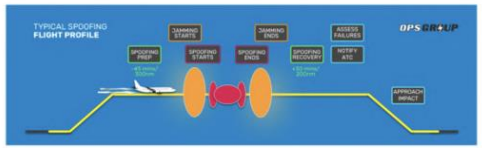
- **Pre-Flight Briefing** Spoofing area locations, intentions, ground-based navaids, likely system losses, indications of spoofing, contingencies/emergencies.
- **Spoofing Maps** - Review
- **GPWS** - Review likely impacts, action plan
- **IRS** Full alignment, manually if in spoofing area
- **Flight Planning** - File on navaid-based airways, review Cb activity (Wx Radar failure), avoid RNP approaches.
- **Sync watches, Check MEL** items, refresh technical understanding,

PRE-SPOOFING

- **Prepare** setup by 45 mins/300nm prior spoofing area
- **Re-Brief Plan** - actions, signs, systems loss
- **Monitor** - EPU/ANP, open sensor/POS REF page, anticipate jamming first, monitor clock.
- **Increase Vigilence -** Unusual system behavior, cross check to handheld GPS, alerting app, ATC reports
- **Set up aircraft systems** - Follow OEM/Opr guidance, de-select GPS to FMS, de-select IRS Hybrid, clock to INT, inhibit EGPWS Look-ahead mode, stow HUD.

IN SPOOFING

- **Aviate, navigate, communicate** - back to basics.
- **Note time** on personal watch, record on log
- **Check system settings** correct for spoof protection
- **Check GPS input** de-selected
- **Check IRS Hybrid mode** de-selected
- **Heading mode** if needed
- **Confirm Nav source** in FMS
- **Report to ATC**, request vectors if needed
- **Inhibit EGPWS** at cruise alt, if procedure allowed



JAMMING Indications

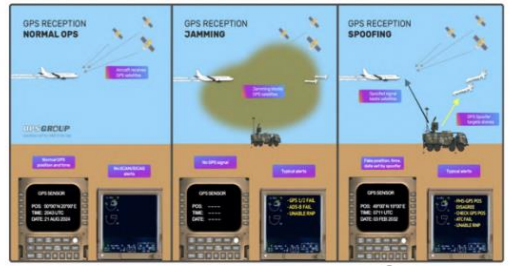
- GPS Failure message
- ADS-B Failure/Warning
- GPWS Terrain caution message
- SATCOM loss
- EGPWS Terrain fail
- Loss of SVS

SPOOFING Indications

- GPS position disagree message
- Rapid EPU/ANP increase
- Aircraft Clock time change
- Transponder fail
- Uncommanded autopilot turn
- Synthetic vision reversion
- Wind indicator illogical
- GPS posn on ND differs from FMS posn
- See full guidance text for complete list

RECOVERY

- **Be certain spoofing finished**
- **Check GPS sensor page** for correct time, date, GS, alt.
- **Assess** all systems for failures
- If allowed, carry out in-flight reset of MMR/GPS/GPWS
- Re-select GPS sensor input to FMS
- Advise ATC of remaining failures
- **Oceanic:** early message to OACC of RNP/CPDLC/ADS-C failures, anticipate lower crossing alt/reroute.
- **Appoach:** Avoid RNP approaches, advise ATC, brief intentions re. EGPWS false alerts, basic modes, possible ECAM/EICAS alerts, check alternates



THREE STAGES FOR ACHIEVING PNT RESILIENCE IN CRITICAL NATIONAL INFRASTRUCTURE

All CNI sectors rely on Position, Navigation, and Timing (PNT) services from satellite systems and other sources. Organisations should develop, implement, and embed a Prepare-Act-Recover PNT resilience framework to ensure systems that rely on PNT services can recover effectively from disruption caused by technological failures, naturally occurring events, or malicious activity.

PREPARE FOR PNT DISRUPTIONS

1. Include PNT resilience in existing governance, cyber-risk, and business continuity frameworks.
2. Test system responses to understand effects of PNT disruptions on system behaviour.
3. Build a mitigation strategy to improve resilience and preserve safety, security and economic performance.

ACT WHEN PNT DISRUPTIONS OCCUR

1. Detect disruption events as soon as possible after they occur.
2. Take planned steps to preserve essential levels of safety, security, and economic wellbeing.
3. Monitor, measure, and record the impact of disruptions on system performance.

RECOVER FROM PNT DISRUPTIONS

1. Return to standard operations when safe and secure to do so.
2. Assess mitigation effectiveness and update response plans and continuity frameworks.
3. Share lessons learned when reporting incidents and their associated impacts.

GET THE PNT RESILIENCE CHECKLIST

Loss of PNT services is now a critical risk on the UK's National Risk Register.

Checklist and resources: www.rin.org.uk/resilient_pnt

Issue 1-00

Self-scoring tools

10 Questions to Gauge Your Organisation's Preparedness

All CNI organisations should assess their preparedness for PNT disruptions. The checklist below will help you to gauge your level of resilience and start to identify gaps to address:

1	Does your organisation maintain a list of all systems (including suppliers) that are connected to, or rely upon, PNT information?	Yes / No
2	Does your organisation maintain a record of why each connected/reliant system needs a source of PNT and what effect the degradation or loss of PNT would have on it?	Yes / No
3	Is the degradation or loss of PNT services (e.g. GNSS) captured on your risk register?	Yes / No
4	Is there a designated person or team within your organisation who is responsible for ensuring the availability and quality of PNT information to all of the systems that require it?	Yes / No
5	Do your critical systems all use multiple independent sources of PNT to remove the risks of single points of failure?	Yes / No
6	Do you have a detailed and documented understanding of how your systems respond to the degradation or loss of PNT information for extended periods of time? *e.g. for 1 minute, 1 hour, 1 day, 1 week, 1 month*	Yes / No
7	Do you have mitigation plans in place for what to do if these systems lose access to PNT for extended periods of time? *e.g. for 1 minute, 1 hour, 1 day, 1 week, 1 month*	Yes / No
8	Do you conduct regular testing on your systems to validate the PNT risks that you have identified and assess the effectiveness of the mitigations you have put in place?	Yes / No
9	Do you have internal roadmaps in place that address improving your resilience to PNT outages as new threats evolve?	Yes / No
10	Does your organisation monitor PNT technology trends and assess when to upgrade its systems as more resilient technologies become available?	Yes / No

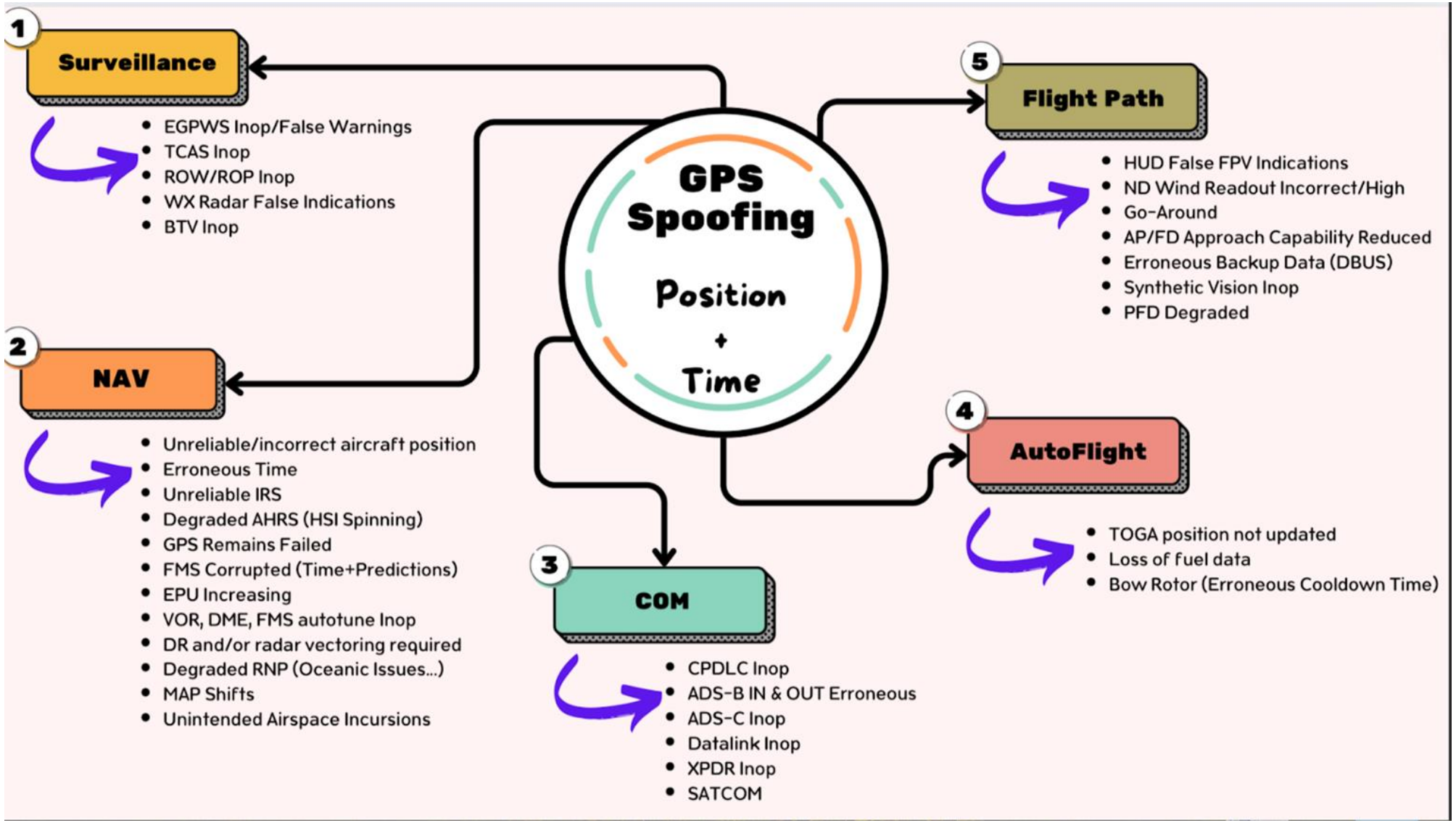
More information: www.rin.org.uk/resilient_pnt

10 Questions to Gauge Your Organisation's Preparedness

All CNI organisations should assess their preparedness for PNT disruptions. The checklist below will help you to gauge your level of resilience and start to identify gaps to address:

1	Does your organisation maintain a list of all systems (including suppliers) that are connected to, or rely upon, PNT information?	Yes / No
2	Does your organisation maintain a record of why each connected/reliant system needs a source of PNT and what effect the degradation or loss of PNT would have on it?	Yes / No
3	Is the degradation or loss of PNT services (e.g. GNSS) captured on your risk register?	Yes / No
4	Is there a designated person or team within your organisation who is responsible for ensuring the availability and quality of PNT information to all of the systems that require it?	Yes / No
5	Do your critical systems all use multiple independent sources of PNT to remove the risks of single points of failure?	Yes / No

OpsGroup report example connectivity map



6	Do you have a detailed and documented understanding of how your systems respond to the degradation or loss of PNT information for extended periods of time? *e.g. for 1 minute, 1 hour, 1 day, 1 week, 1 month*	Yes / No
7	Do you have mitigation plans in place for what to do if these systems lose access to PNT for extended periods of time? *e.g. for 1 minute, 1 hour, 1 day, 1 week, 1 month*	Yes / No
8	Do you conduct regular testing on your systems to validate the PNT risks that you have identified and assess the effectiveness of the mitigations you have put in place?	Yes / No
9	Do you have internal roadmaps in place that address improving your resilience to PNT outages as new threats evolve?	Yes / No
10	Does your organisation monitor PNT technology trends and assess when to upgrade its systems as more resilient technologies become available?	Yes / No

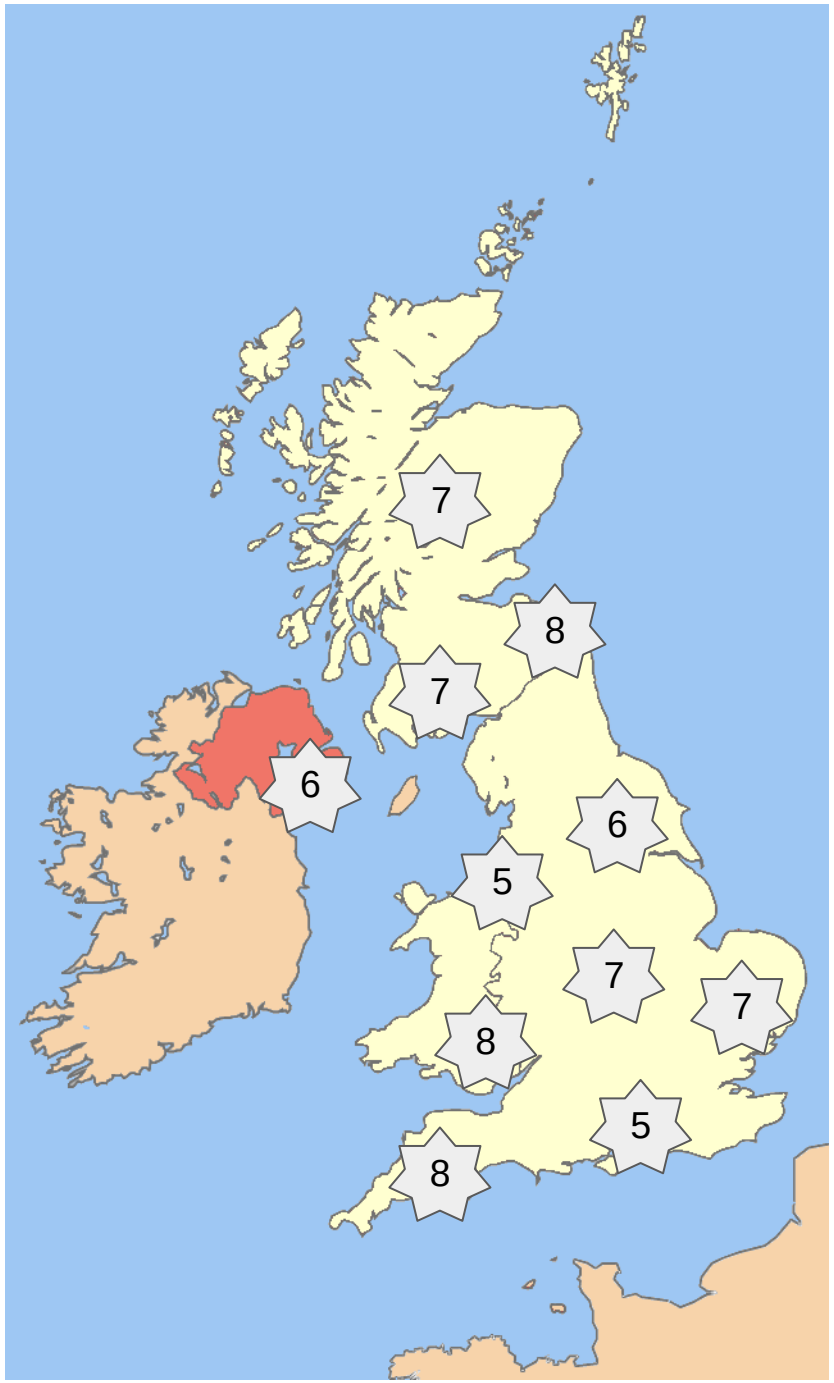
More information: www.rin.org.uk/resilient_pnt

6	Do you have a detailed and documented understanding of how your systems respond to the degradation or loss of PNT information for extended periods of time? *e.g. for 1 minute, 1 hour, 1 day, 1 week, 1 month*	Yes / No
7	Do you have mitigation plans in place for what to do if these systems lose access to PNT for extended periods of time? *e.g. for 1 minute, 1 hour, 1 day, 1 week, 1 month*	Yes / No
8	Do you conduct regular testing on your systems to validate the PNT risks that you have identified and assess the effectiveness of the mitigations you have put in place?	Yes / No
9	Do you have internal roadmaps in place that address improving your resilience to PNT outages as new threats evolve?	Yes / No
10	Does your organisation monitor PNT technology trends and assess when to upgrade its systems as more resilient technologies become available?	Yes / No

More information: www.rin.org.uk/resilient_pnt

Resilience checklist

- Scope for providing KPIs or similar metric to help assess how the UK's providers for any given sector/CNI are faring
- Scope for a multi-year "getting to ten" strategy for resilient PNT for each CNI
- Can help with gap analyses in existing/ongoing programmes



Example mitigation plan

Example mitigation plans for a fleet of delivery drivers serving a supermarket using a company-provided satnav for all navigation, planning, and communication					
	Disruption type				
Outage period	PNT system has lost power	Communication link lost	Physical damage to PNT system	Poor terrestrial/space weather degrading PNT	PNT device is suffering electronic interference
1 minute	Pull over when safe to verify physical connections	Continue operations and monitor comms link	Use paper maps or a backup system (e.g. personal smartphone)	Be aware of the expected degradation in PNT performance	Wait to see if the interference passes
1 hour	Use paper maps or a backup system (e.g. personal smartphone)	Continue operations and monitor comms link	As above	Be aware of the expected degradation in PNT performance	Look for signs of interference on board the vehicle, e.g. unusual electronics being carried aboard
1 day	Request replacement and use a temporary portable satnav device until repaired	Plan all routes and delivery schedules on paper in advance each day	Replace the PNT system	Be aware of the expected degradation in PNT performance	Request the use of a different vehicle which does not suffer the same interference
1 week	As above	As above and move to alternative communications link	As above	Be aware of the expected degradation in PNT performance	Change journey routes to avoid the interference if it is a regional problem.Use paper maps and alternative PNT sources that do not suffer the interference
1 month	As above	As above	As above	Be aware of the expected degradation in PNT performance	Change journey routes to avoid the interference if it is a regional problem.Use paper maps and alternative PNT sources that do not suffer the interference

Example mitigation plan

Example mitigation plans for a fleet of delivery drivers serving a supermarket using a company-provided satnav for all navigation, planning, and communication					
	Disruption type				
Outage period	PNT system has lost power	Communication link lost	Physical damage to PNT system	Poor terrestrial/space weather degrading PNT	PNT device is suffering electronic interference
1 minute	Pull over when safe to verify physical connections	Continue operations and monitor comms link	Use paper maps or a backup system (e.g. personal smartphone)	Be aware of the expected degradation in PNT performance	Wait to see if the interference passes
1 hour	Use paper maps or a backup system (e.g. personal smartphone)	Continue operations and monitor comms link	As above	Be aware of the expected degradation in PNT performance	Look for signs of interference on board the vehicle, e.g. unusual electronics being carried aboard
1 day	Request replacement and use a temporary portable satnav device until repaired	Plan all routes and delivery schedules on paper in advance each day	Replace the PNT system	Be aware of the expected degradation in PNT performance	Request the use of a different vehicle which does not suffer the same interference
1 week	As above	As above and move to alternative communications link	As above	Be aware of the expected degradation in PNT performance	Change journey routes to avoid the interference if it is a regional problem.Use paper maps and alternative PNT sources that do not suffer the interference
1 month	As above	As above	As above	Be aware of the expected degradation in PNT performance	Change journey routes to avoid the interference if it is a regional problem.Use paper maps and alternative PNT sources that do not suffer the interference

Example mitigation plan

Example mitigation plans for a fleet of delivery drivers serving a supermarket using a company-provided satnav for all navigation, planning, and communication					
	Disruption type				
Outage period	PNT system has lost power	Communication link lost	Physical damage to PNT system	Poor terrestrial/space weather degrading PNT	PNT device is suffering electronic interference
1 minute	Pull over when safe to verify physical connections	Continue operations and monitor comms link	Use paper maps or a backup system (e.g. personal smartphone)	Be aware of the expected degradation in PNT performance	Wait to see if the interference passes
1 hour	Use paper maps or a backup system (e.g. personal smartphone)	Continue operations and monitor comms link	As above	Be aware of the expected degradation in PNT performance	Look for signs of interference on board the vehicle, e.g. unusual electronics being carried aboard
1 day	Request replacement and use a temporary portable satnav device until repaired	Plan all routes and delivery schedules on paper in advance each day	Replace the PNT system	Be aware of the expected degradation in PNT performance	Request the use of a different vehicle which does not suffer the same interference
1 week	As above	As above and move to alternative communications link	As above	Be aware of the expected degradation in PNT performance	Change journey routes to avoid the interference if it is a regional problem.Use paper maps and alternative PNT sources that do not suffer the interference
1 month	As above	As above	As above	Be aware of the expected degradation in PNT performance	Change journey routes to avoid the interference if it is a regional problem.Use paper maps and alternative PNT sources that do not suffer the interference

Example mitigation plan

Example mitigation plans for a fleet of delivery drivers serving a supermarket using a company-provided satnav for all navigation, planning, and communication					
	Disruption type				
Outage period	PNT system has lost power	Communication link lost	Physical damage to PNT system	Poor terrestrial/space weather degrading PNT	PNT device is suffering electronic interference
1 minute	Pull over when safe to verify physical connections	Continue operations and monitor comms link	Use paper maps or a backup system (e.g. personal smartphone)	Be aware of the expected degradation in PNT performance	Wait to see if the interference passes
1 hour	Use paper maps or a backup system (e.g. personal smartphone)	Continue operations and monitor comms link	As above	Be aware of the expected degradation in PNT performance	Look for signs of interference on board the vehicle, e.g. unusual electronics being carried aboard
1 day	Request replacement and use a temporary portable satnav device until repaired	Plan all routes and delivery schedules on paper in advance each day	Replace the PNT system	Be aware of the expected degradation in PNT performance	Request the use of a different vehicle which does not suffer the same interference
1 week	As above	As above and move to alternative communications link	As above	Be aware of the expected degradation in PNT performance	Change journey routes to avoid the interference if it is a regional problem.Use paper maps and alternative PNT sources that do not suffer the interference
1 month	As above	As above	As above	Be aware of the expected degradation in PNT performance	Change journey routes to avoid the interference if it is a regional problem.Use paper maps and alternative PNT sources that do not suffer the interference

Summary

The UK has launched Best Practice Guidelines for Resilient PNT aimed at Critical National Infrastructure operators and suppliers

The “Principles on a page”, a supporting website, and a set of tools and example materials are currently available

The Royal Institute of Navigation will continue to update the materials and hold workshops with each of the UK CNI through 2025

Feedback is greatly appreciated!

Thanks to all involved

Core Working Group Members

Richard Bowden, Guy Buesnel, Mitch Narins, John Pottle, Andy Proctor

Review committee and advisors

Martin Bransby, Nigel Davies, Tony Flavin, Alan Grant, Paul Groves, Stephen Hancock, Leon Lobo, Paul Osborn, David Politt, Dan Tillett, Yeqiu Ying

UK PNTO and DSIT

Dozens of UK CNI representatives and reviewers