GPS Spoofing

FINAL REPORT

OF THE GPS SPOOFING WORKGROUP

Technical Analysis & Impact

Flight Crew Guidance

Safety Concerns

Solutions

Recommendations

GPS Spoofing WorkGroup

OPSGROUP

September 6, 2024

Created by the 950 participants of the GPS Spoofing Workgroup 2024.

Published by OPSGROUP,
September 6th, 2024.

Enquiries: gps@ops.group.

Contents

GPS Spoofing: Technical Guide

Impacts

Safety Concerns

Crew Guidance

Solutions

Recommendations

Appendix

Key Findings

- Overall, the Workgroup assessed that the impact of GPS Spoofing on flight safety, aircraft operation and handling, and ATC operations, is **extremely significant**. Beyond this report, the topic requires considerable further industry analysis and attention, particularly in the domain of flight safety, to avoid serious incidents and accidents.

- The workgroup is very concerned about the overall impact of GPS Spoofing on **flight safety**. A total of 8 overall safety concerns, and a further 33 specific concerns were raised, including: Aircraft operation and handling (11 concerns), EGPWS (8 concerns), Procedures and training (4 concerns), Human factors and CRM (6 concerns), Air Traffic Control (4 concerns).

- The greatest safety concern is the degraded functionality of the **Ground Proximity Warning System (GPWS).** The system does not operate correctly after spoofing, even if GPS coverage is restored. The number of false alerts is astounding. There is an increasing normalization of risk. As a result, there was widespread apprehension in the Workgroup that the decades-long work to reduce Controlled Flight Into Terrain (CFIT) accidents is at great risk of being undone.

- A similar concern is the significant possibility of the GPS Receiver **appearing normal** to flight crew after spoofing, but in reality being contaminated with false data. This places doubt on the use of GPS at any point after spoofing, especially RNP approaches, and RNP enroute use.

- This year, a 500% increase in spoofing has been observed. On average 1500 flights per day are now spoofed, versus 300 in Q1/Q2 of 2024. This is coincident with the summer months in spoofing affected areas. **With winter approaching**, the operating environment changes from predominantly good weather and VMC conditions, to poor weather, icing, and IMC conditions. **This change will increase the risk factors significantly.**

- From the flight crew perspective, the Workgroup noted a lack of availability of **technical information** on GPS involvement in aircraft systems, conflicting crew guidance, and incomplete or insufficient procedures, all leading to misunderstandings and knowledge gaps.

- **The future of GPS use in aviation is unclear**. The Workgroup assessed that the vulnerabilities in public-use GPS that are now becoming evident (although known to experts for a decade or more), mean that the high involvement of GPS in aircraft systems is a **major issue**. Further, the over-reliance on GPS for primary navigation places great importance on preserving a sufficient network of conventional ground-based navaids. This aspect of the issue requires deeper study and conversation.

- A survey of flight crew was carried out as part of the Workgroup. The response was excellent – almost 2,000 completed surveys were returned to the Workgroup. The results show that a full **1,400 crew members** (~70%) rated their concern relating to GPS Spoofing impact on flight safety as **very high or extreme**. 91% of all crew members rated their concern as moderate or higher.

- The Workgroup noted many **misconceptions about the reason** GPS Spoofing is occurring. With few exceptions, GPS Spoofing is conducted by state actors as a result of regional conflict. The Workgroup found no examples of a direct, targeted attack on a civilian aircraft.

- In broad terms, **there are no quick and easy solutions**. The key focus in the short term is on mitigation, crew awareness, guidance, and training. In the longer term, the Workgroup identified potential solutions to hardware, avionics and system components.

- Consideration must be given to the potential for a **deepening of the GPS vulnerability problem**. In mid-2024, we are already seeing a major increase in both spoofing, and impact to aircraft. Locations could widen further, and impacts could worsen.

A Community Effort ...

Everything you see in this report is the result of community effort. If you know OPSGROUP, you know that this is our approach to solving problems in international flight operations.

We have a strong, safety-focused industry, but sometimes things come up that affect us all, yet can't be solved by an individual aviation authority or group. GPS Spoofing is one such "thing".

This WorkGroup was truly something special. The participation of 950 individual people, across the entire industry – pilots, ATC, authorities, manufacturers, GPS experts, industry groups - is a marker of how much concern there is about the GPS Spoofing problem. But participation is just the first step. What stands out in this WorkGroup is the above-and-beyond efforts from so many participants.

Seemingly confounding technical questions were answered quickly, data was offered, contacts were sourced, ideas and solutions were hammered out into the small hours. For six weeks, we worked weekends and late nights, and no stone remained unturned. The energy, drive, and commitment of so many to solve this many-headed Hydra never faded.

There is so much knowledge, experience, and expertise in the international ops community, along with the key ingredient: a desire to share our skills, to tell each other what may harm us, to lead groups and to push for change. It's amazing to see.

Thank you to everyone who took part. From here, we hope that our efforts lead to better-informed flight crews, attention on the safety risks we have listed, and consideration of the recommendations presented at the end of this report.

Mark Zee,
CEO & Founder, OPSGROUP.

Special Thanks ...

The WorkGroup would like to recognize and thank in particular the following people for their support, expertise, enthusiasm, and drive to make this WorkGroup a tremendous success.

Ramsey Faragher (Royal Institute of Navigation), Bulent Atas (Turkish Airlines), Jeremy Bennington (Spirent), Matt Berthet (Corsair), Agustin Boehler (Copa Airlines), Benjamin van der Sanden and Philippe Domogala (IFATCA), Martin Laplante (Bombardier), Gerhard Berz (Eurocontrol), Capt. Hovav Ben David (El Al), Aleks Kowalski (BALPA), Maxime Wauters (EBAA), Agata Burek (SkyTaxi), Werner Heumann (Emirates), Sajeel Akhtar (Avion Express), Andriy Kostyuk (Azerbaijan Airlines), George Chiotis (Etihad), Nikola Cojic (IFATSEA), Dominic Waeckerlin (SwissAvTech), Tim Morton, James Pyne (Embraer), Gian Andrea Bandieri (EASA), Paul Martin (Civil Aviation Authority of Singapore), Jacob Young (NATS UK), Angelina Jacobson (FAA), Raoul van Mil (ECA/IFALPA), Daniel Aisen (Turkish Airlines), Ken Alexander (FAA), Tom Gooch (Omni Air), Evangelos Antonopoulos (DCA Cyprus), Tom Kirkhope (UK CAA), Mitch Narins (Strategic Synergies, LLC), Steve Thorpe (NBAA IOC), Stephane De Wolf (IBAC), Jake Zettwoch (UPS), Steve Hammack (Honeywell), Nikolay Dimitrov (Air Canada), John Foley (Garmin), and especially the team at Zurich University of Applied Sciences and SkAI Data Services: Benoit Figuet, Michael Felux and Raphael Monstein.

The Workgroup also gratefully acknowledges the support and assistance of the Israel National Cyber Directorate, the UK MOD, the UK Royal Air Force (RAF), NASA, U.S. Space Command, EASA, BALPA, the Dutch VNV, SITA, Honeywell, Aircraft Performance Group, FlightSafety International, and the University of Texas.

A special thank you to the WorkGroup Team Leaders for Technical, Mitigation, Safety, Solutions, and Research: Bulent Atas, Matt Berthet, Michael Felux, André Bos, Werner Heumann, Stephen Smartt, Ramsey Faragher, Okuary Osechas, Tom Kirkhope, Angelina Jacobson, Agustin Boehler, and Joaquim Mestre.

Thank you also to the almost two thousand flight crew and aircraft operator personnel that completed the GPS Spoofing WorkGroup Survey.

Participants

Aaron Adams ■ Aaron Pycraft ■ Abdelrahman Aljarrah ■ Abheepsa Gupta ■ Abhinav Gahlaut ■ Adam Pitchford ■ Adharan Paul ■ Adrian Stefan ■ Adrian Tickle ■ Adriano Pittalis ■ Adriano Schembri ■ Adrianus Brobbel ■ Agata Burek ■ Ágúst Kolbeinsson ■ Agustin Boehler ■ Ahmad Waheed ■ Ahmed Boufares ■ Ahmet Ilkay Yigit ■ Ajay Goyat ■ Ajay Rajbanshi ■ Akashdeep Kaul ■ Akshay Dewan ■ Al Evans ■ Alaa El Dine Schiff ■ Alan Grech ■ Alan Nala ■ Alan Stewart ■ Alasdair Heneghan ■ Alberto Lopez Quintana ■ Alberto Valentini ■ Aldo Stefanon ■ Alecyr Monteiro Cruz ■ Aleix Canet ■ Aleks Kowalski ■ Alessandro Conte ■ Alex Plachkov ■ Alexander Merkt ■ Alexander Visser ■ Alexandre Leiria ■ Alexandre Lenoble ■ Alexis Clere ■ Ali Razi ■ Allen Ratterree ■ Almerindo Miguel ■ Alon Refaeli ■ Alvaro Neves ■ Amar Murthy ■ Amelia Rahmawaty ■ Amir Hyster ■ Amy Kiiru ■ Anant Patel ■ Anders Nissen Mosegaard ■ André Bos ■ Andre de Chauvigny de Blot ■ Andre Hansen ■ Andre Minella ■ Andre Reed ■ Andrea Kayson ■ Andrei Necuta ■ Andrew Burke ■ Andrew Drake ■ Andrew Elbert ■ Andrew Evlambides ■ Andrew Hart ■ Andrew Karas ■ Andrew King ■ Andrew Kovats ■ Andrew Krites ■ Andrew Samuel ■ Andrew Sibenaler ■ Andrew Stukey ■ Andrew Waber ■ Andriy Kostyuk ■ Andy Hoag ■ Andy Keiser ■ Andy Skinner ■ Andy Spencer ■ Angelina Jacobson ■ Anne Mackenzie ■ Anthony Ngu ■ Anthony Seely ■ Anton Troskie ■ Antonia Ivan ■ Antonio Colo ■ Antonio Correas ■ Arnaud Thurat ■ Arnis Kadakovskis ■ Arnoldo Pieper ■ Arthur Marim ■ Asef Jahmani ■ Ashwin Thomas ■ Ateeq Siddiqi ■ Austin Albright ■ Ayhan Demir ■ Ayman Hassan ■ Balthasar Indermuehle ■ Barış Eren ■ Barry Comerford ■ Ben Beaumont ■ Ben Rosinger ■ Benedict Khoo ■ Benjamin Pletcher ■ Benjamin Steen ■ Benjamin van der Sanden ■ Benn Clemence ■ Benoit Figuet ■ Bernd Wiesensee ■ Bernhard Franke ■ Bert Leijen ■ Bert Tompkins Jr ■ Bharat Keswani ■ Bill Young ■ BJ Ferro ■ Bjarney Jensdottir ■ Bob Gasko ■ Bob Owsley ■ Boby Jacob ■ Boris Wong ■ Borja Alomar ■ Brad Robinson ■ Brad Stowe ■ Brandan Madson ■ Brendan Carroll ■ Brenton Skinn ■ Brett Abbott ■ Brian Buescher ■ Brian Dana ■ Brian Greene ■ Brian Pullin ■ Brian Smith ■ Briano Santos ■ Brigitte Fromm ■ Bruce Anderson ■ Bryan Berkbigler ■ Bryan Colombo ■ Bryan Hecker ■ Bryan Turner ■ Buket Celik ■ Bulent Atas ■ Bulent Ince ■ Callum Best ■ Carey Miller ■ Carl Dobbs ■ Carl Sange ■ Carlos Pi Cubi ■ Carlos Sousa ■ Carlos Tomas Castillo ■ Cataldo De Benedittis ■ Catherine Graham ■ Cathy Vienneau ■ Chakri Thanapprapasr ■ Charalambos Franceskides ■ Charles Kibby ■ Charles Swain ■ Chenglan Wang ■ Cherie Thompson ■ Chiaki Yokota ■ Chris Bernal ■ Chris Brault ■ Chris Burden ■ Chris Caine ■ Chris Chop ■ Chris Devine ■ Chris Opris ■ Chris Shieff ■ Chris Stephan ■ Chris Stiffler ■ Chris Volonakis ■ Chris West ■ Christian Ramsey ■ Christina Clausnitzer ■ Christoffer Linden ■ Christophe De Bacquer ■ Christopher Jason ■ Christos Vasileiadis ■ Christy DeYoung ■ Christy Hickey ■ Chuck Stoffer ■ Claudia Cabaço ■ Clint El-Ramey ■ Colin Russell ■ Colin Warner ■ Connor Brokaw ■ Conor Barrett ■ Corinne Lefebvre ■ Craig Bowers ■ Craig Erickson ■ Craig Homer ■ Craig Van Deventer ■ Crystal Tse ■ Cuong Quach ■ Cyril Deroyer ■ Cyrille Aubergier ■ Cyrille Rosay ■ Damian Cross ■ Damian Fong ■ Dan Cooke ■ Dan Johnson ■ Dan Miller ■ Dan Paulk ■ Dan Richards ■ Dana Goward ■ Danial Rahim ■ Daniel Aisen ■ Daniel Ayotte ■ Daniel Chiommino ■ Daniel Fleming ■ Daniel Folie ■ Daniel Hinkel ■ Daniel Jansen ■ Daniel Keller ■ Daniel Poit ■ Daniel Roberts ■ Daniele Travaglia ■ Danijel Kecman ■ Dario Santagati ■ Darrell Pennington ■ Dave Andrews ■ Dave Steinbrunner ■ David Andrews ■ David Bjellos ■ David Crettenand ■ David Fletcher ■ David Gray ■ David Mumford ■ David Rogers ■ David Sánchez-Heredero ■ David Schöne ■ David Thompson ■ David Trickey ■ David Wightman ■ David Woodcock ■ Dean Fontenot ■ Denis Kimani ■ Derek Fleck ■ Desmond Ross ■ Devrim Cagdas ■ Dheeraja Nayak ■ Dhirender Bhardwaj ■ Diego Albert ■ Dirk Eger ■ DJ Judkins ■ Djani Bodlovic ■ Dominic Waeckerlin ■ Dominik Harrer ■ Donald Kolbus ■ Doug Cassaro ■ Doug Shields ■ Doug Walsh ■ Drew May ■ Duane Giorgetti ■ Eamonn Riley ■ Ed Hahn ■ Eduardo Moreira Lopes ■ Eduardo Stocker ■ Ehsen Qureshi ■ EJ Hendrickson ■ Elionor Payeras Martorell ■ Elize van Ingen Lambermont ■ Ellen McGaughy ■ Elson Foo ■ Emmajane Bremner ■ Emre Battal ■ Eric Becktell ■ Eric Dalton ■ Eric Goodman ■ Eric Rossignol ■ Erik Drobny ■ Eriva Randriamanjatosoa ■ Espen Jakobsen ■ Ethan Ceresney ■ Etienne Côté ■ Evan Mccarthy ■ Evangelos Antonopoulos ■ Fabio Pallone ■ Fadi Khalil ■ Fahad AlMannaei ■ Faria Habbash ■ Fed Silvestri ■ Federico Bevilacqua ■ Federico Orta ■ Felix Manso Fernandez ■ Fern Campos ■ Fernando Riet ■ Filip Bujoczek ■ Florian Buchmann ■ Francisco Gallardo ■ Francisco Herrera ■ Francisco Martinez ■ Franco Salluce ■ Francois Debrouwere ■ Frank Cruz ■ Frank Flood ■ Frank Neumann ■ Frank Salfner ■ Frederick Sossaman ■ Gangadharan Pradeep ■ George Chiotis ■ George Foo ■ George Heavers ■ George Hunter ■ Gerald Campbell ■ Gerard Rene Peacock ■ Gerhard Berz ■ Germán García González ■ Gian Andrea Bandieri ■ Gilles Cochet ■ Ginny Spicer ■ Glenn McDermott ■ Gökalp Günes ■ Gopitha Ranasinghe ■ Graeme Pollard ■ Grant Russell ■ Greg Dyer ■ Greg Meech ■ Greg Pleinis ■ Gregor Burkhard ■ Gregory Delbeke ■ Guillaume Obry ■ Gunnar Ingi Briem ■ Gunther Pott ■ Gus Ortiz ■ Gustavo Salinas ■ Gyorgy Peto ■ Hamdi Nasser ■ Hanna Hirschfeld ■ Hannes Hesshaimer ■ Hans Mueller ■ Hans Pfeiffer ■ Harald Lazar ■ Haris Antoniades ■ Harry Tzonos ■ Hassan Serghini ■ Hector Falcon ■ Heine Lykke Korreborg ■ Helena Azevedo ■ Hennie Joubert ■ Herbert Naef ■ Hielke Brouwer ■ Hovav Ben David ■ Hugo Lücke ■ Iain Brown ■ Ian Petchenik ■ Ian Roy ■ Iason Rigas ■ Ignacio Tobias ■ Ihsan Serdar Micozkadioglu ■ İshakbeyoğlu Süleyman ■ Islam Elsayed ■ Ivan Semaka ■ Jack Tacchino ■ Jacob van Eldik ■ Jacob Young ■ Jacopo Sagone ■ Jade Allouche-Rongeon ■ Jake Zettwoch ■ Jakob Engelbrecht ■ James Andrews ■ James Aviles ■ James Booth ■ James Boston ■ James Iannotta ■ James Miller ■ James Pyne ■ James Storey ■ James Toye ■ James Wootton ■ Jamie Rose ■ Jamie-Lee Torrance ■ Jan Kupzog ■ Jane Ross ■ Janelle Schultz ■ Janis Krupins ■ Jared Falcon ■ Jared Hill ■ Jason Brownell ■ Jason Lim ■ Jason Nygren ■ Jason Redenius ■ Jean Marcellin ■ Jean-Emmanuel Cau ■ Jeff Baber ■ Jeff Brooks ■ Jeff Gibbs ■ Jeff Jerman ■ Jeff Ryan ■ Jeff Stanley ■ Jeff Uekert ■ Jeffery Sanders ■ Jeffrey Bennett ■ Jeffrey Bryant ■ Jeffrey Coon ■ Jennafer Cohrs ■ Jeremy Konis ■ Jeremy Pickles ■ Jérôme Tuaillon ■ Jesse Nanninga ■ Jhanica Almario ■ Jill Wittels ■ Jim Alexander ■ Jim Gautrey ■ Jim Malzone ■ Jimmy Dailey ■ Jimmy Tan ■ Jo-elle Van Epps ■ Joaquim Mestre ■ Jocelyn Descaillot ■ Joe Naughton ■ Joe Opaski ■ Joe Sears ■ Joel Davis ■ Joel Knisely ■ Joel Levasseur ■ Johan Gauermann ■ Johan Schneider ■ Johan Westin ■ John Edmonds ■ John Foley ■ John Hutchison ■ John Lawson ■ John Sweet ■ John Weidner ■ John Wells ■ John Wiseman ■ Jonatan Meschke ■ Jonatas Magalhaes ■ Jonathan Gordon ■ Jonathan Hecker ■ Jonathan Witten ■ Jonathan Yancey ■ Jonathan Zarinnia ■ Jorge Parada ■ Joris Van den Branden ■ José Azevedo ■ Jose Lopez ■ Jose Luis Allo

■ Joseph Agius ■ Joseph Duval ■ Joseph Griggs ■ Joseph Henson ■ Joseph Pereira ■ Josh Keep ■ JP Du Toit ■ Julia Harvey ■ Julian Oehling ■ Julien Roquoplo ■ Julio Montalvo ■ Jun Cai ■ Justin Brown ■ Justin Webb ■ Justin Williams ■ Kabir Singh ■ Kai Odenthal ■ Kaitlyn Moyer ■ Kalaichelvan Many ■ Kamran Gill ■ Karsten Liljegren ■ Kathrin Borwig ■ Keith Carlyle ■ Kelene Fercho ■ Kelvin Chan ■ Kemalcan Aygül ■ Ken Alexander ■ Ken Hanson ■ Ken McNeil ■ Ken Ozkaptan ■ Ketill Gunnarsson ■ Kevin Bachner ■ Kevin Baldock ■ Kevin Glynn ■ Kevin MacMillan ■ Kevin Walsh ■ Khalid Pervaiz ■ Kilian Dolan ■ Kirsten Drost ■ Koen Scheers ■ Krasimir Hristov ■ Krikor Michikian ■ Kyle Colasanto ■ Kyle Smalling ■ Kyle Zerkel ■ Lair Souza ■ Lamar Strachan ■ Laura Chappell ■ Laura Meier ■ Laurent Vialard ■ Lawrence Tochukwu Ejezie ■ Len LeCompte ■ Leo De Cristofano ■ Leo Kotil ■ Leonardo Goncalves ■ Leonardo Lima ■ Leonardo Sanches e Souza ■ Leonardo Utsch ■ Leonie Löffler ■ Lindsey Krebs ■ Lisa Dyer ■ Loise Mwangi ■ Lorenzo Key ■ Lou Courey ■ Louise Bullen ■ Lovro Grlj ■ Luca Fratini ■ Luca Versetti ■ Lucy Youdell ■ Luis Rueda ■ Luka Pace Bonello ■ Lukas Mayer ■ Makiko Tokumoto ■ Malcolm Budd ■ Manas Mukherjee ■ Manish Makhija ■ Manuel Cuntz ■ Manuel Heinz ■ Manuel Malaure ■ Manuel Vindas ■ Marcel Seybal ■ Marcelo Alencar ■ Marco Beuker ■ Marco Ghelardi ■ Marcos Domínguez Suárez ■ Marcus Graham ■ Maria Choi ■ Maria Sweeney ■ Marijs Kolenberg ■ Mark Evers ■ Mark Hurston ■ Mark Mckee ■ Mark Morrison ■ Mark Roman ■ Mark Semon ■ Mark Shurville ■ Mark Zee ■ Mark Zuranski ■ Markus Schmidt ■ Markus Wildner ■ Marnix van 't Hoff ■ Martin Kemp ■ Martin Laplante ■ Martin laplante ■ Martin Luton ■ Martin Scepan ■ Martin Wasserbauer ■ Marty Rollinger ■ Marwan AlMasri ■ Massimiliano Civettini ■ Matt Berthet ■ Matt Gee ■ Matt Harty ■ Matt McAleer ■ Matthew Dietz ■ Matthias Naupold ■ Matthias Schäfer ■ Matthieu Durand ■ Matthieu Evain ■ Maurizio Colombo ■ Max Calnin ■ Maxence Heldenbergh ■ Maxime Boyer-Beaucage ■ Maxime Wauters ■ Melody Shaffer ■ Michael Cook ■ Michael Felux ■ Michael Guenthner ■ Michael Jessup ■ Michael Jones ■ Michael Lebovitz ■ Michael Nikolic ■ Michael Perry ■ Michael Sherwood ■ Michael Van der Klip ■ Michael Vaughan ■ Michel Roelandt ■ Michele Carandente ■ Mick Campbell ■ Miguel Martin ■ Mika Hissa ■ Mike Abajian ■ Mike Boyd ■ Mike Brown ■ Mike Lawson ■ Mike Meraviglia ■ Mike Payne ■ Mike Rotko ■ Mike Shama ■ Mike Sundsted ■ Milud Bakkar ■ Mimmo Catalano ■ Mitch Narins ■ Mladen Simovic ■ Mohamed Alnoaimi ■ Mohamed Altalibi ■ Mohamed Chahid ■ Mohamed Sary ■ Mohammad Al Tal ■ Mouhcine Souabni ■ Mourad Ben Asker ■ Muhammad Ehtasham ■ Muhammad Ghani ■ Mukesh Sehgal ■ Mukul Garg ■ Murat Gezeravci ■ Naomi Schayek ■ Narayan Dhital ■ Nat Iyengar ■ Nathan Richards ■ Nathan Wiesenfeld ■ Naveen Supramaniam ■ Nazim Belhannache ■ Neil Naik ■ Neil Singer ■ Nick Cook ■ Nick Freeman ■ Nick Jackereas ■ Nicolas Horn ■ Nicolas Mejia ■ Nicolas Roisne ■ Niels Mikkelsen ■ Nigel Rosendale ■ Nik Dimitrov ■ Nikhil Mathen ■ Nikhilesh Bauri ■ Niklas Ahrens ■ Nikola Cojic ■ Nikolaj Petersen ■ Nikolaos Koukouvaos ■ Nikolay Dimitrov ■ Nitin Sabherwal ■ Noah Trent ■ Noel Dwyer ■ Noud Schoffelmeer ■ Oguz Dalbeyler ■ Okuary Osechas ■ Ole Fisker ■ Oleksandr Lisniak ■ Olga Itenberg ■ Oliver Klumaier ■ Oliver Regehr ■ Olivia Koski ■ Olugbenga Oluwasanmi ■ Oren Eshet ■ Orhan Acar ■ Ori Gross ■ Osama Alhayek ■ Osama Khan ■ Oscar de Rojas ■ Owen McAree ■ Panayiota Spyrou ■ Pat Cassidy ■ Pat Nadeau ■ Patrick Byrne ■ Patrick Engling ■ Patrick Jordan ■ Patrick Liu ■ Patrick Richards ■ Paul Carroll ■ Paul Harrison ■ Paul Lee ■ Paul Martin ■ Paul McKee ■ Paul Nguyen ■ Paul Rodell ■ Paul Wigginton ■ Paul Zuccarelli ■ Paulo Fonseca ■ Pedro Amorim ■ Pedro Cardoso ■ Pedro Correia ■ Pedro Nunes ■ Pedro Velez ■ Peron Taitt ■ Peter Baranko ■ Peter Brangam ■ Peter Douet ■ Peter Gear ■ PH Chan ■ Philip Kanonis ■ Philipp Rudnik ■ Philippe Birkel ■ Philippe Domogala ■ Poul Lind ■ Prashant Prabhakar ■ Prateek Singh ■ Preston Williamson ■ Quentin Cortese ■ Radi Radi ■ Rafa Bajares ■ Rafael Bessa ■ Rafael Chepote ■ Rafal Marczewski ■ Raj Kumar ■ Rajneesh Sharma ■ Ramsey Faragher ■ Randy Rufi ■ Raoul van Mil ■ Raphael Monstein ■ Raul Montano ■ Ravi Bajaj ■ Ray Johnson ■ Razvan Berla ■ Reggie Beaudoin ■ Reggie Redetzke ■ Reinhard Michel ■ Remilekun Etta ■ Reto Portmann ■ Reza Ali ■ Ricardo Arcaini Da Silva ■ Ricardo De Sousa ■ Richard DeMaria ■ Richard Hayward ■ Richard Snyder ■ Richard Vosburg ■ Richard Yeates ■ Rick Niles ■ Rick Travis ■ Riley McNay ■ Rino Finamore ■ Robbie Shakespeare ■ Robert Fleming ■ Robert Garner ■ Robert Giles ■ Robert Hoffman ■ Robert Hummel ■ Robert McDonald ■ Robert Russell ■ Robert Spurlock ■ Robert Vriesman ■ Rodger Horton ■ Rodney Griffing ■ Rodrigo Barradas ■ Roger Cox ■ Roger Pierce ■ Rohan Perera ■ Rohit Malhotra ■ Roman Aryond ■ Roman Dzivy ■ Ron Baker ■ Ron Nelson ■ Ron Unruh ■ Ronald Ledany ■ Ronald Weber ■ Rory Bertram ■ Ross Dawson ■ Rustom Kapadia ■ Ryan Goheen ■ Ryan Meeks ■ Ryan Retelle ■ Ryan Teo ■ Sacha Rossi ■ Saikat Das ■ Sajeel Akhtar ■ Sajin Mohamed ■ Sameer Kapoor ■ Sammi Foy ■ Sandeep Sandhu ■ Sandeep Tyagi ■ Sandro Oberoi ■ Sanjiv Sabarwal ■ Sarah Jeziorski ■ Savvas Theodoulou ■ Scott Bergstrom ■ Scott Buethe ■ Scott Johnson ■ Scott Owens ■ Scott Ragone ■ Scott Sims ■ Seamus Flannery ■ Sean Wahl ■ Sebastian Gosch ■ Sebastian Hudemann ■ Sebastian Joseph ■ Sebastien Robert ■ Sebastien Seykora ■ Seif Gharbi ■ Selva Ganesh ■ Serdar Sahin ■ Sergey Nartov ■ Sergey Sokolov ■ Sergio Hernandez ■ Seth Moffat ■ Seyed Saanei ■ Shane Nicholson ■ Sharad Goswami ■ Sharon Anderson ■ Shaun ONeal ■ Shawn Mechelke ■ Shelagh Milne ■ Shelby King ■ Shelley Perry ■ Shem Malmquist ■ Sherry Borener ■ Shihhsuan Wang ■ Shingai George ■ Sidra Jabeen ■ Sierra Garber ■ Silvia Hernandez ■ Silvia Neves ■ Simon Eardley ■ Simon Michaelson ■ Simona Blaskova ■ Sisay Befekadu ■ Sonny Lokhoff ■ Sorawat Prasongdee ■ Spenser Phillips ■ Sreenath Nair ■ Stefan Hageneier ■ Stefan Holmgren ■ Stefano Biundo ■ Stephane Beauchamp ■ Stephane De Wolf ■ Stephen Campos ■ Stephen Creamer ■ Stephen Hartley ■ Stephen Hutchins ■ Stephen Smartt ■ Steve Hammack ■ Steve Hutchins ■ Steve McFerrin ■ Steve Morais ■ Steve Shiveley ■ Steve Thorpe ■ Steve Tripp ■ Steven Brandt ■ Steven Hoffman ■ Stu Cox ■ Stuart Rankin ■ Suneet Krishna ■ Suresh Madhuram ■ Susan Maddigan ■ Suzanne Snygg ■ Sven Slattberg ■ Sylvain Cuerrier ■ Ta Quoc Viet ■ Tahir Ozceik ■ Tahir Semih Ozcelik ■ Tamir Goren ■ Tefho Keothepile ■ Terrence Muir ■ Thaddeus Beebe ■ Theo Hankers ■ Thibault Delassus ■ Thomas Frei ■ Thomas Walther ■ Thorsten M Hagel ■ Ti Zhang ■ Tiago Ferreira ■ Tim Morton ■ Tim Radigan ■ Tim Steffen ■ Tim Young ■ Timo Heinze ■ Timo Klippel ■ Timothy Pedley ■ Timur Dubovik ■ Titipong Buddeesuwan ■ Todd Chisholm ■ Todd Hoisington ■ Todd Siegel ■ Todd Studer ■ Tom Gooch ■ Tom Irbinger ■ Tom Kirkhope ■ Tom Koss ■ Tom Newman ■ Tomas Correa ■ Tomislav Dunderovic ■ Tomonorl Tsuruzono ■ Tony Antoniou ■ Tony DiVerniero ■ Travis Moore ■ Trenton Kessler ■ Trey Turner ■ Tyler Mosset ■ Udhana Abeysekera ■ Umair Bhutto ■ Utsav Mukhopadhyay ■ Uwe Goehl ■ Uwe Nitsche ■ Vaughn Gruneberg ■ Velislav Kostov ■ Veselin Popovic ■ Vikram Pant ■ Viktor Jagasits ■ Vinayak V P ■ Vincent Hubert ■ Viraaj Shah ■ Vivian Chua ■ Vladimir Ojeda ■ Volker Stuhlsatz ■ Walter Kraujalis ■ Warwick Stone ■ Wayne Snyder ■ Wei Jen Tan ■ Werner Heumann ■ William Ellis ■ William Geiser ■ William Prokop ■ Xavier Collin ■ Yann Poudoulec ■ Yariv Tawil ■ Yaron Marom ■ Yavuz Barbaros Ulusoy ■ Yeray Gonzalez ■ Yoahann Banaji ■ Yohannes Seifu ■ Yoni Malka ■ Yosef Seyfu ■ Yousif Alsaad ■ Yunus Emre Ozturk ■ Zach Clements ■ Zbig Jasiukajc ■ 950 amazing people: **thank you**.

GPS Spoofing

Why, where, how.

GPS spoofing began to severely impact civil aviation in September 2023. While GPS interference is not a new phenomenon, the scale and effects of the current wave of spoofing are unprecedented.

In the first few months, relatively few aircraft were affected, but by January 2024, an average of 300 flights a day were being spoofed. By August 2024, this had grown to around 1500 flights per day.

Most recently, for the one-month period from July 15 - August 15, 2024, a total of 41,000 flights experienced spoofing.

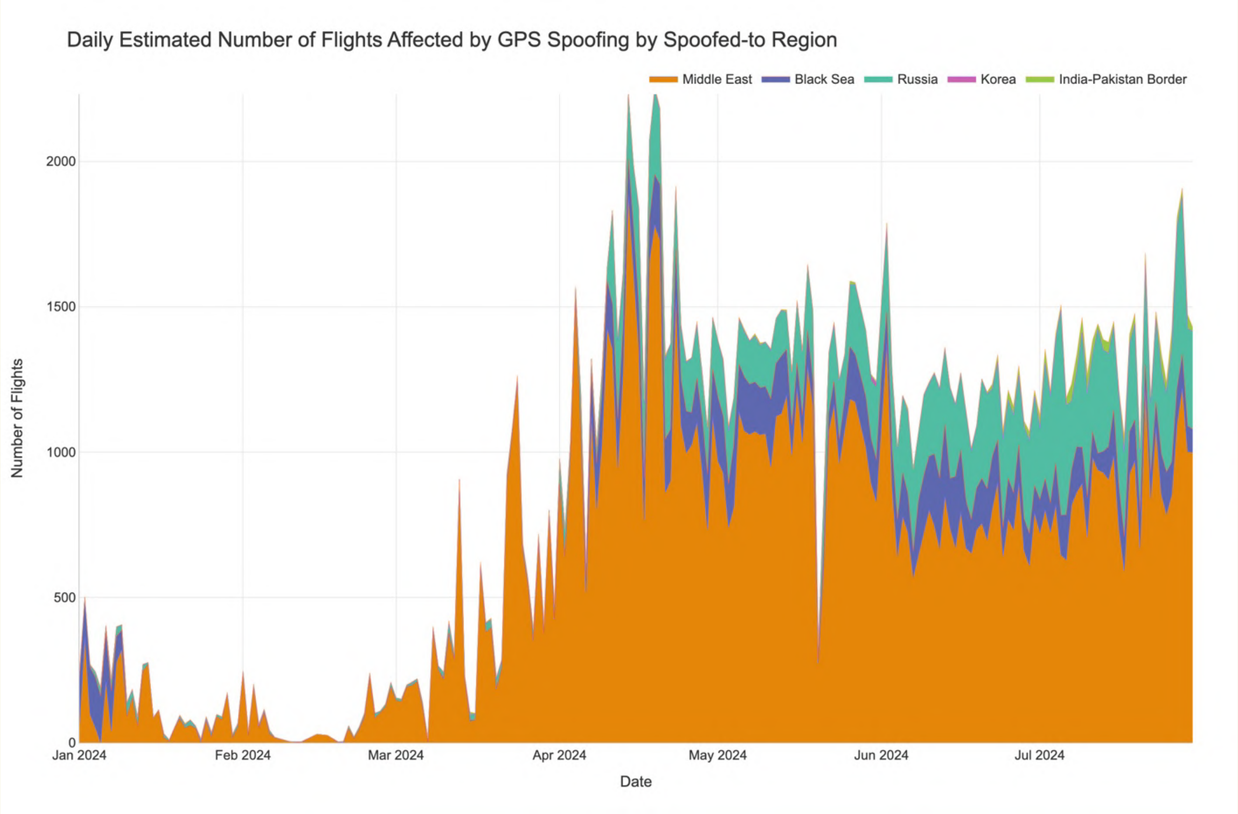
Because modern aircraft have incorporated GPS into a large number of aircraft systems, the impact of a spoofed GPS signal has had severe and cascading effects. These include the FMS, Hybrid IRS, the aircraft clock, GPWS, Weather Radar, CPDLC, ADS-B and ADS-C, as well as numerous other systems.

This section of the report will provide a technical overview of the reasons for spoofing, methodology, locations, and current trend.

Major increase in spoofing in 2024

This chart shows the daily number of estimated spoofed flights per falsified location.

A clear rise in spoofing incidents is evident from April 2024 onwards, based on algorithms applied to ADS-B data. Not all spoofing can be detected this way; the true number could be significantly higher.



Data source: ZHAW/SkAI Data Services, using the OpenSky Network.

Why is GPS Spoofing happening?

Almost all current GPS spoofing incidents currently affecting civil aircraft are related to conflict zones.

Spoofing is a very effective mechanism to counter drones, which are increasingly used in modern warfare. Spoofing platforms and devices are operated by military units.

These signals used to counter drones, and disrupt/confuse other GPS receivers, are also being picked up by civil aircraft.

There is no evidence, so far, to suggest that civil aircraft are being deliberately targeted.

Primary actors currently carrying out GPS Spoofing

- Military units targeting hostile drones, and drone swarms, in conflict zones (e.g., Israel, Ukraine, Russia).

- Military units acting on behalf of the state, disrupting shipping (e.g., Crimea, Black Sea)

- Military units disturbing the flight path of other GPS-guided ammunition, missiles, or vehicles (autonomous or manned).

Other actors

- Police, Public Safety and National Security agencies preventing drone use at events (e.g., Euro 2024, Olympics), borders, and sensitive areas. They often use counter-drone systems to jam or spoof GPS to force drones to land.

- Commercial drivers (truck, taxi) may use jamming or spoofing to interfere with their reported locations, but there is no verified current impact on civil aviation from these.

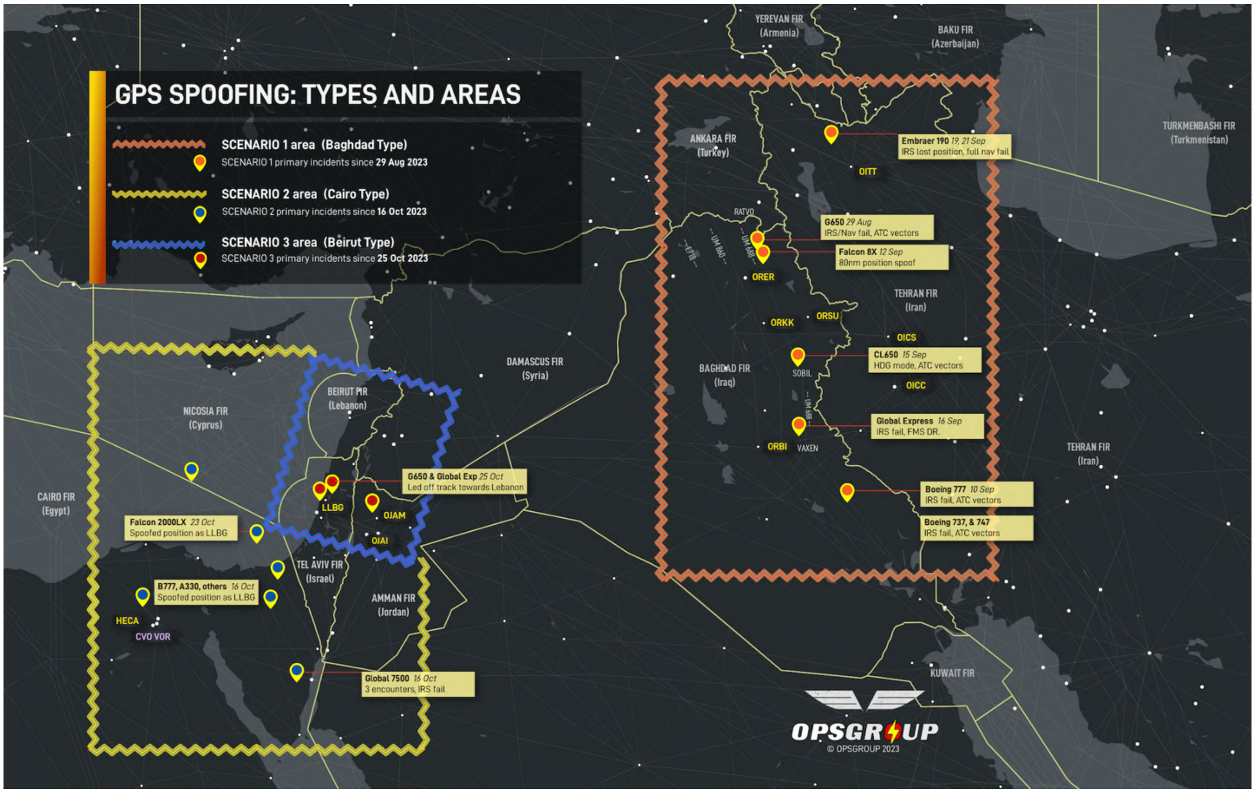
Where is GPS Spoofing happening?

GPS Spoofing is currently concentrated in **very specific areas near conflict zones**. The highest level of spoofing is in the eastern Mediterranean, near Israel, Lebanon, Cyprus and Egypt. Other areas of significant spoofing include the Black Sea, western Russia, and the India/Pakistan border. Complete maps are shown in the next section.

History and Locations

The first series of GPS Spoofing events took place in September 2023 in the area of northern Iraq, centered on Baghdad. Approximately 20 aircraft reports were received by OPSGROUP, with similar patterns of system behavior: navigation position uncertainty, FMS degradation, apparent IRS failures. Some aircraft were left unable to navigate independently after the spoofing event, requiring ATC vectors. Aircraft clocks were showing wrong times.

By November 2023, 50 reports had been received by OPSGROUP with further spoofing locations being noted in the Eastern Mediterranean, centered on Cairo, Tel Aviv and Beirut.

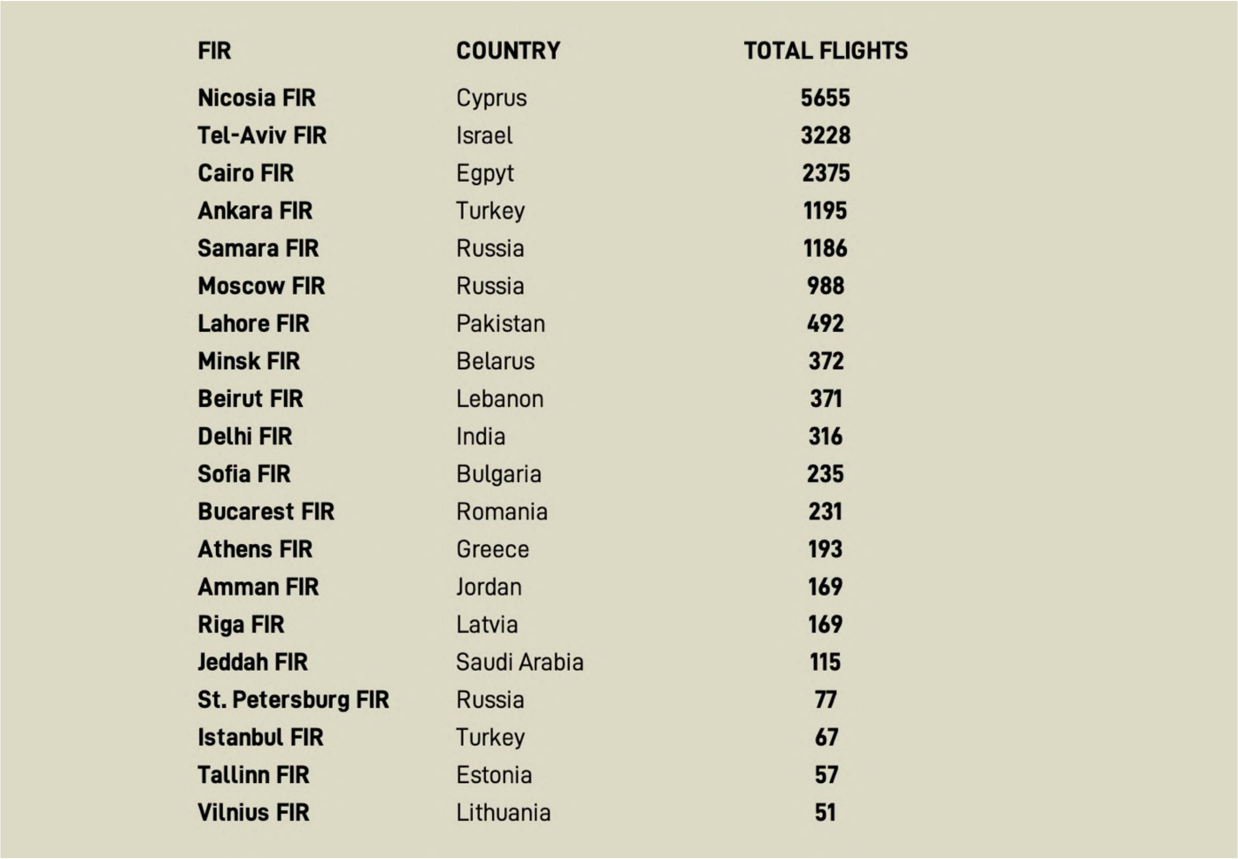


Initial GPS Spoofing locations, as at November 2023. Source: OPSGROUP.

During 2024, as employment of spoofing tactics by military forces widened, new spoofing locations were identified in the Black Sea region, western Russia and the Baltics, North/South Korea border areas, western Ukraine, and the India/Pakistan border.

Spoofing by Flight Information Region (FIR)

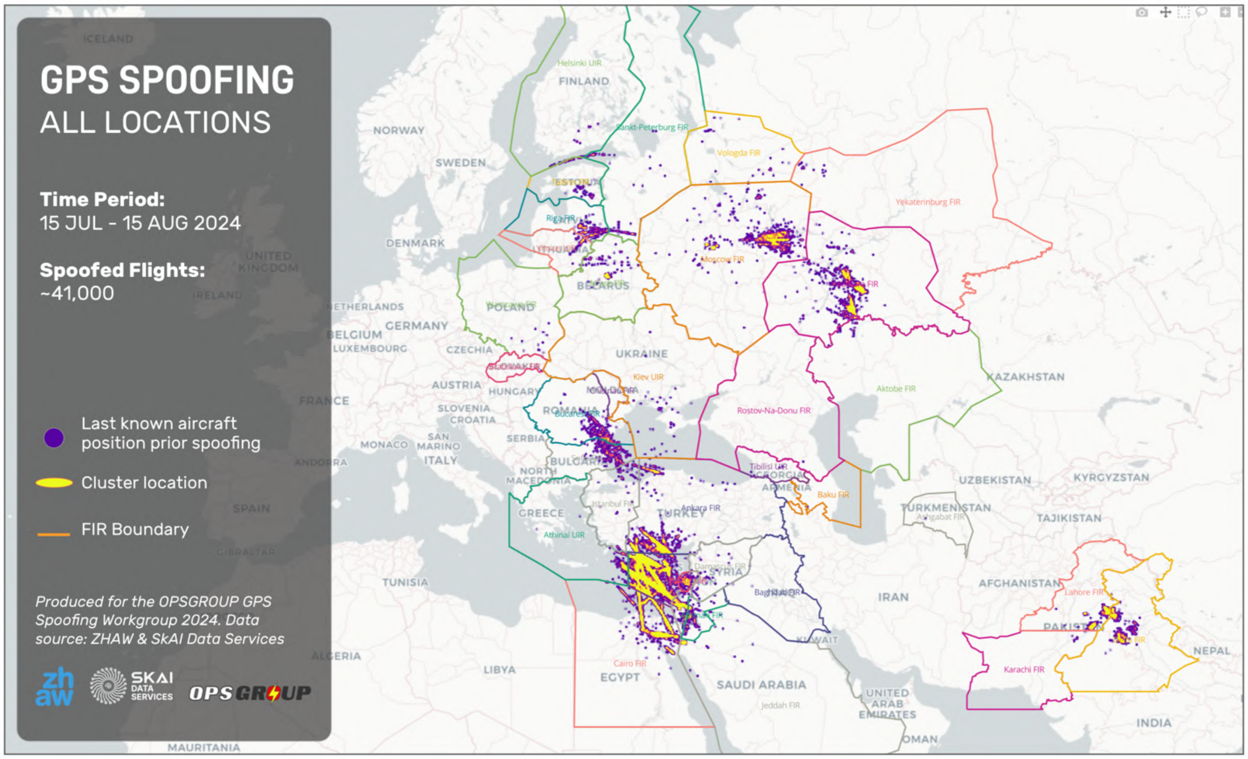
The table below shows the number of aircraft impacted by spoofing in the Top 20 FIR's affected, during the period July 15 – August 15.



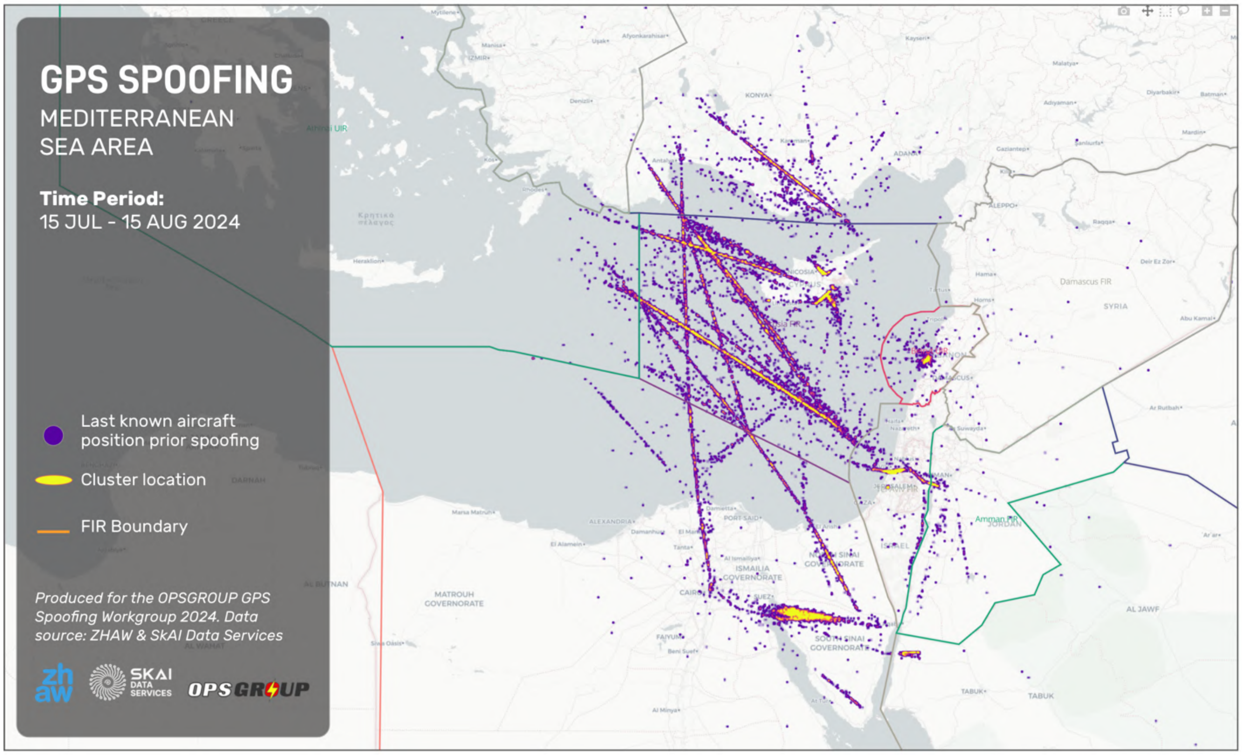
FIR	COUNTRY	TOTAL FLIGHTS
Nicosia FIR	Cyprus	**5655**
Tel-Aviv FIR	Israel	**3228**
Cairo FIR	Egpyt	**2375**
Ankara FIR	Turkey	**1195**
Samara FIR	Russia	**1186**
Moscow FIR	Russia	**988**
Lahore FIR	Pakistan	**492**
Minsk FIR	Belarus	**372**
Beirut FIR	Lebanon	**371**
Delhi FIR	India	**316**
Sofia FIR	Bulgaria	**235**
Bucarest FIR	Romania	**231**
Athens FIR	Greece	**193**
Amman FIR	Jordan	**169**
Riga FIR	Latvia	**169**
Jeddah FIR	Saudi Arabia	**115**
St. Petersburg FIR	Russia	**77**
Istanbul FIR	Turkey	**67**
Tallinn FIR	Estonia	**57**
Vilnius FIR	Lithuania	**51**

Table: Number of spoofed flights by Flight Information Region (FIR), taken from data for the period July 15 - August 15, based on last known position before spoofing. Note that not all flights can be traced to a last known position due to GPS Jamming preceding the spoofing event. Only 17,000 of the 41,000 flights spoofed in this period are included in this data. However, the data does give a good representation of the most affected FIR's. Source: ZHAW/SkAI Data Services.

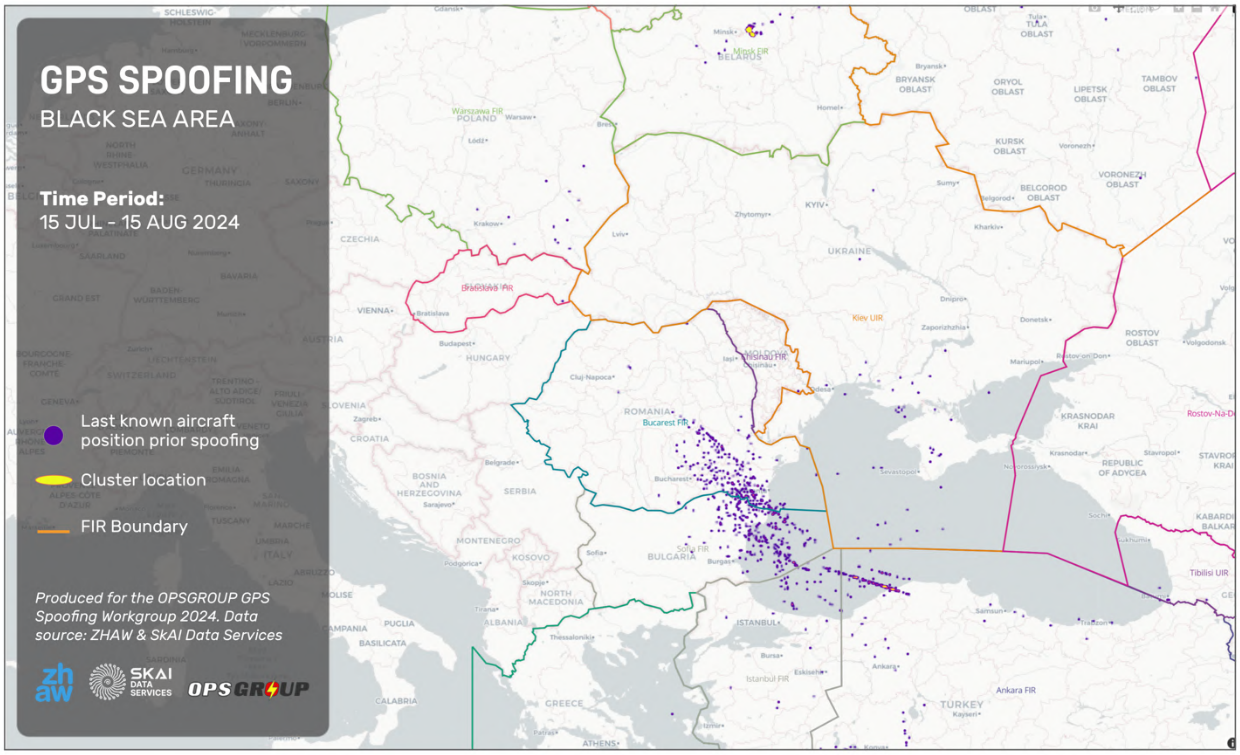
Location Maps



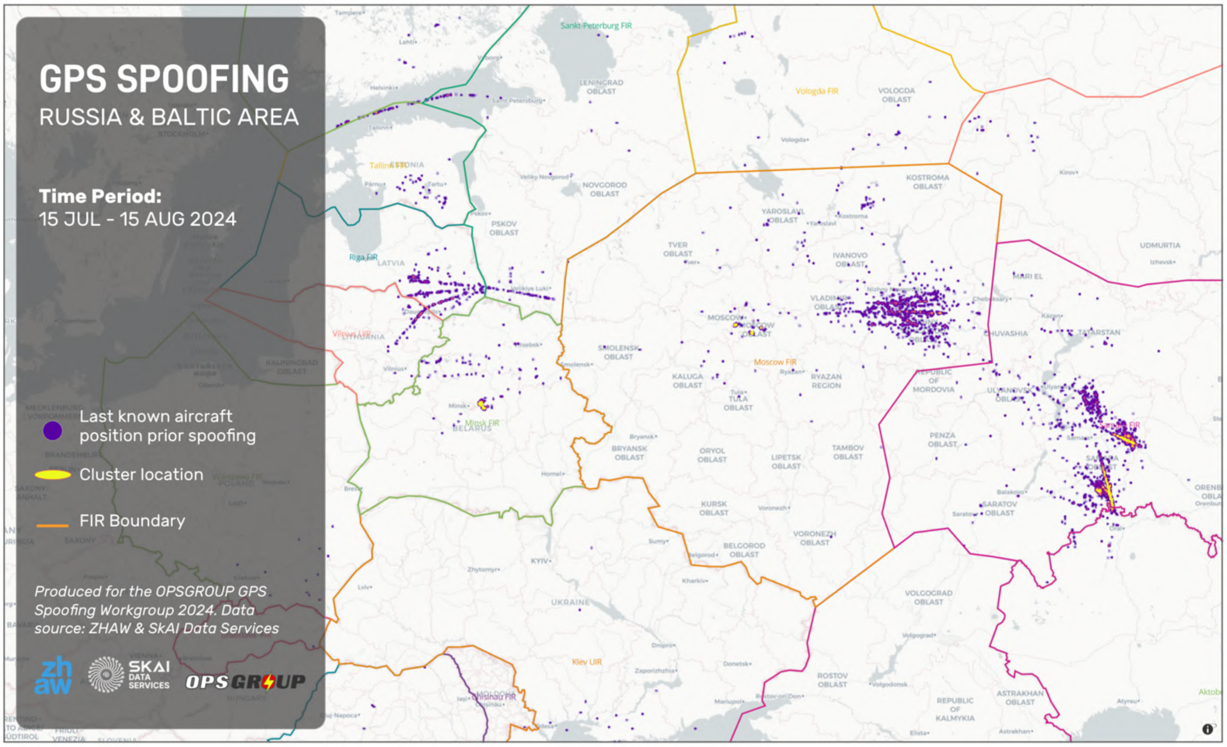
Map: All worldwide spoofing locations, August 2024. See Appendix for full map catalogue.



Map: Mediterranean Sea area, August 2024. See Appendix for full map catalogue.



Map: Black Sea area, August 2024. See Appendix for full map catalogue.



Map: Russia & Baltic area, August 2024. See Appendix for full map catalogue.

Spoofing detailed by region

As of August 2024, the following are the **major spoofing areas** worldwide. Locations can change without notice, but all these regions have had steady spoofing impact throughout 2024.

1. Eastern Mediterranean Sea area

Nicosia FIR - Cyprus. Currently the highest spoofed FIR worldwide. Spoofing related to Israel conflict. All routes, entire FIR. Includes approaches to LCLK/Larnaca and on-ground spoofing. Spoofed-to position was mostly OLBA/Beirut; as of August 24, 2024, that changed to mostly OJAI/Amman.

Beirut FIR – Lebanon. Entire FIR. Traffic into OLBA/Beirut airport is regularly spoofed, and on-ground spoofing is common. IRS alignment issues noted. Go-arounds common due to system issues on approach.

Tel Aviv FIR – Israel. Entire FIR at risk of spoofing. LLBG arrivals/departures affected, caution wayward SID tracking and proximity to danger and military areas. On-ground spoofing possible.

Cairo FIR – Egypt. Especially over Sinai Peninsula, north-eastern portion of the FIR, and at Cairo airport. Spoofed-to positions include Beirut, Tel Aviv, Cairo, and Amman. On-ground spoofing possible at HECA/Cairo. Airways L550, L560 most affected, also A16, and any traffic within 200nm of CVO (Cairo) VOR.

Jeddah FIR – Saudi Arabia. Traffic routing to/from Egypt is usually spoofed close to Cairo FIR boundary. Airway/position. Spoofed-to positions include Beirut, Tel Aviv, Cairo, and Amman. Airways L550, L560, UB411 (which carry high levels of east-west traffic) most affected.

Amman FIR – Jordan. Traffic landing at Jordanian airports (OJAM/Amman Marka, OJAI/Queen Alia, OJAQ/Aqaba) regularly spoofed, causing issues with RNP approaches. Entire FIR carries spoofing risk.

2. Black Sea area

Ankara/Istanbul FIRs - Turkey. High levels of spoofing on the northern Turkish coastline, and the western Black Sea area, near Istanbul. Airways UM859, UN743, UL746 most affected. Spoofing here is more commonly preceded by jamming. Spoofed-to position mostly Simferopol airport (Crimea). A second spoofed-to position near Krasnodar identified in June 2024. Region active since March 2024.

Sofia FIR - Bulgaria. Spoofing active in overwater areas in the east of the Sofia FIR, and over land close to the Black Sea coastline, in the area of Burgas and Varna. Affects mostly transit traffic EU-Asia. Spoofed-to position mostly Simferopol.

Bucharest FIR – Romania. South-east quadrant of the FIR sees 90% of the spoofing, in the area between Brasov, Bucharest and Constanta. Affects mostly transit traffic EU-Asia. Spoofed-to position mostly Simferopol.

3. Russia & Baltic region

Samara & Moscow FIRs - Russia. Hotspots are Nizhny Novgorod and Samara, with high levels of spoofing in these areas. Spoofed-to locations show Moscow and Yaroslavl.

Tallinn, Riga and Vilnius FIRs – Estonia, Latvia, Lithuania. Spoofing most noted in the eastern parts of Riga FIR (Latvia) and Vilnius FIR (Lithuania). Airway M864 is the most affected. Spoofed-to location typically Smolensk.

Helsinki FIR – Finland. Spoofing is most common on the Helsinki/Tallinn FIR boundary, mostly used by Russian aircraft transiting to Kaliningrad, but also noted around EFLA/Lahti and EFHK/Helsinki. Spoofed-to location is Smolensk.

4. India/Pakistan border

Lahore & Delhi FIRs – Pakistan & India. Daily spoofing has been occurring here since May 2024. Areas north-west of New Delhi, and in the area of Lahore, are the most affected. Spoofed-to locations generally along the line of the border.

Previous spoofing locations

Iraq, Iran (Baghdad and Tehran FIRs). Initially a major location, now minor. In the first wave of GPS Spoofing incidents, 80% were occurring in an area between ORBI/Baghdad airport and the northern ORBB/Baghdad FIR boundary, and close to the Iranian border (OIIX/Tehran FIR). Sporadic/occasional spoofing seen again August 2024.

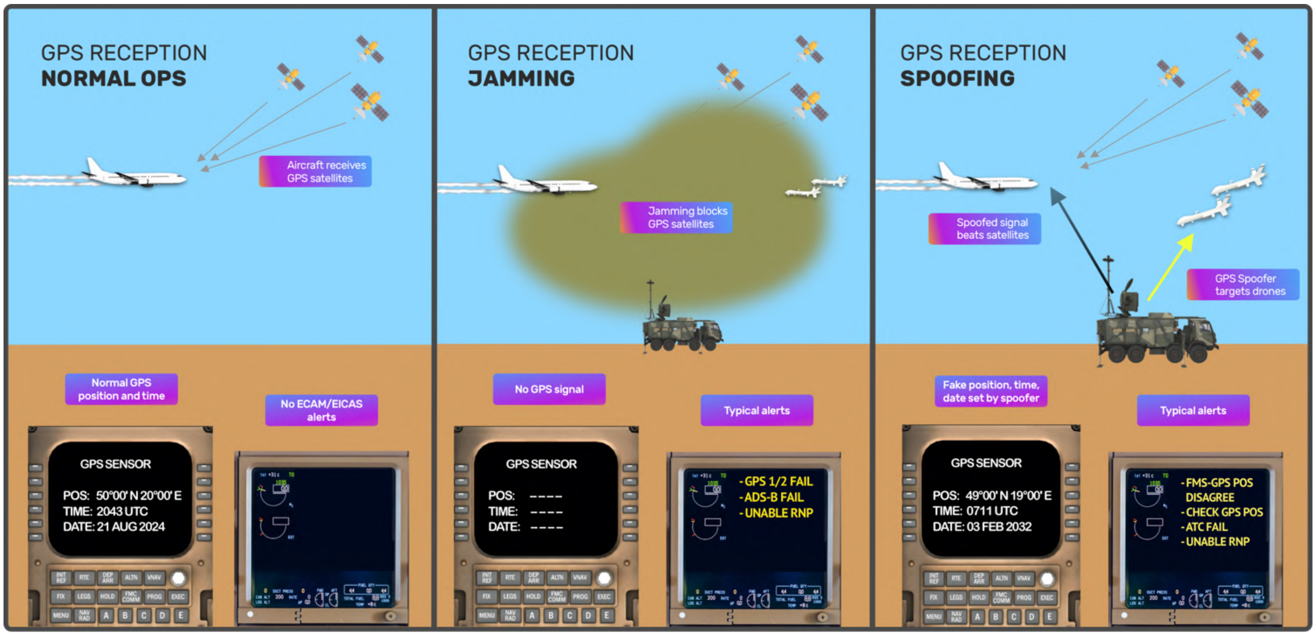
North/South Korea (Pyongyang and Incheon FIRs). A period of GPS Spoofing was recorded in June 2024. The majority occurred near the North/South Korean border. A small number of spoofing incidents seen in the oceanic portion of the FIR.

China. A number of reports, and correlated data, showed spoofing near Beijing airport in May 2024. No recent reports.

How GPS Spoofing works

In **normal operation**, the aircraft GPS Receiver receives Position, Navigation, and Timing information from a constellation of satellites.

In the **spoofing situations** now commonly encountered, a ground-based spoofing platform broadcasts **fake signals**, which are interpreted as valid by the aircraft GPS receiver. False position and time information is then fed from the GPS receiver to other aircraft systems.



GPS Reception during normal ops, jamming, and spoofing. Larger version in Appendix. Image source: OPSGROUP.

During **GPS Jamming**, a radio transmitter, generally ground-based, transmits noise or interference on the GPS frequency band(s). As a result, the aircraft GPS receiver loses the satellite signal.

During **GPS spoofing**, another ground-based transmitter (or group of transmitters) begins to send a fake GPS signal, causing GPS receivers to calculate incorrect position, time, and altitude. Since satellite signals are very low power, the spoofed GPS signal overpowers these quite easily. The aircraft GPS receiver now takes the fake signal as true, and begins to share the new false position with aircraft systems.

For most spoofing affecting civil aviation at present, these jamming and spoofing transmitters are high-grade military equipment, either portable on a vehicle, or moveable units installed at fixed locations. An example is the Russian spoofing platform on an oil rig in the Black Sea, destroyed by Ukraine in early August 2024 (see "Equipment types" later in this report for more detail).

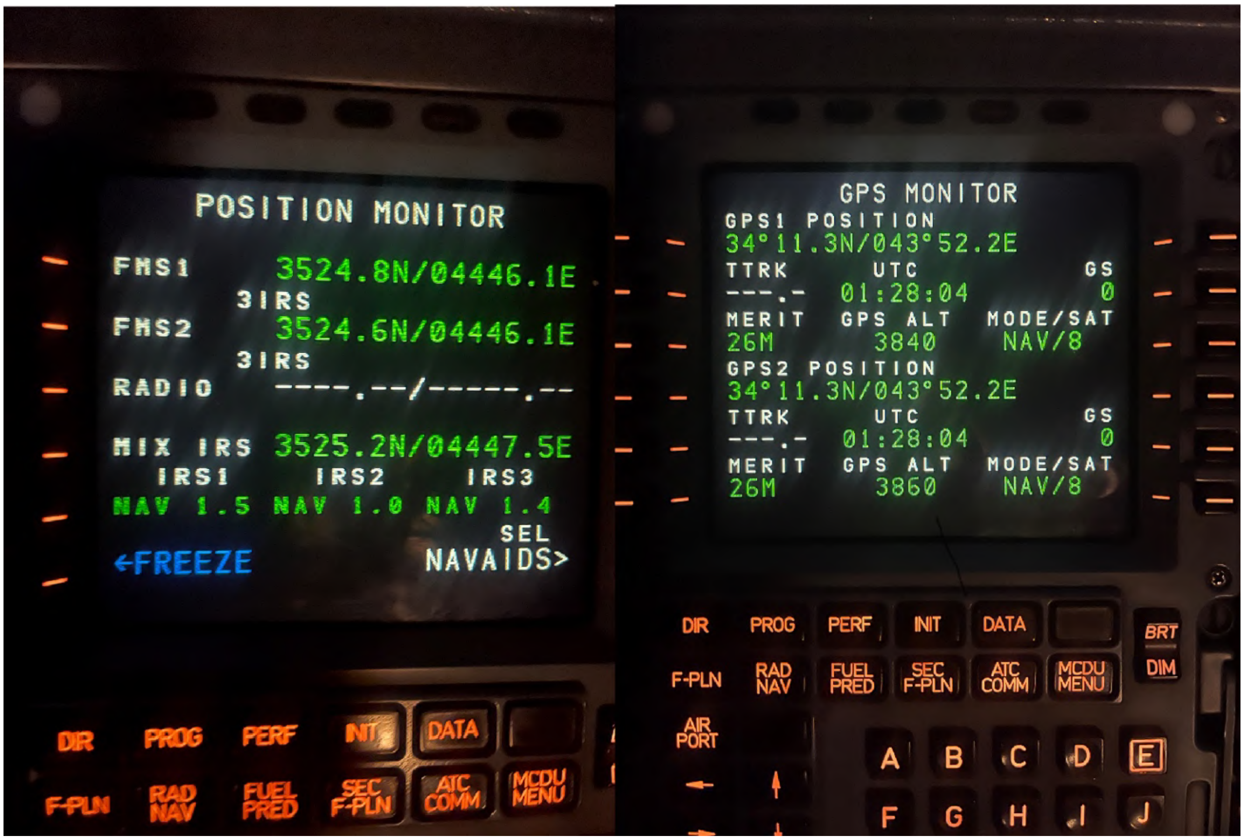
Although these counterfeit signals resemble the genuine signal, they may differ in various ways to fool the GPS receiver:

- Code (and carrier) phase drift

- Altered navigation data: incorrect orbit biases that alter the position completely, or setting some or all satellites to unhealthy.

- Incorrect timestamps broadcast from each satellite. Since a GNSS receiver calculates a spacetime coordinate and a velocity, a spoofer can force a receiver to calculate the wrong position, altitude, speed, time, and date.

An effective method of spoofing receivers with no inherent spoofer protections involves broadcasting a jamming signal that overpowers the existing real signals coming from space ("raising the signal noise floor") and then broadcasting "louder" (but not too loud) spoofing signals on top of this. This causes the true signals from space to get "buried" and the only signals that the receiver will be able to find and decode are the spoofer signals. The receiver will still calculate a signal to noise ratio that is sensible, even though the actual signal powers are much higher than the real ones from space.



```
POSITION MONITOR
FMS1       3524.8N/04446.1E
              3IRS
FMS2       3524.6N/04446.1E
              3IRS
RADIO      ----.--/-----.--

MIX IRS    3525.2N/04447.5E
   IRS1       IRS2      IRS3
NAV 1.5   NAV 1.0   NAV 1.4
                         SEL
<FREEZE             NAVAIDS>
```

```
         GPS MONITOR
GPS1 POSITION
34°11.3N/043°52.2E
TTRK       UTC              GS
---.-    01:28:04            0
MERIT    GPS ALT     MODE/SAT
26M        3840         NAV/8
GPS2 POSITION
34°11.3N/043°52.2E
TTRK       UTC              GS
---.-    01:28:04            0
MERIT    GPS ALT     MODE/SAT
26M        3860         NAV/8
```

An example of GPS Spoofing in action during cruise phase: FMS position shows correct, GPS is being spoofed. Note also GPS Altitude incorrect, True track (TTRK) and Ground Speed (GS) values are zero - all indications of spoofing. A320, ORBB FIR.

Terminology: GNSS vs GPS

Though technically inaccurate, the terms GPS and GNSS are used interchangeably in the aviation industry. GNSS (Global Navigation Satellite System) is an umbrella term covering any satellite constellation that provides positioning, navigation, and timing (PNT) services, and includes Satellite Based Augmentation Systems (SBAS), such as the US Wide Area Augmentation System (WAAS) and the European Geostationary Navigation Overlay System (EGNOS).

The four main GNSS systems in use today are GPS (USA), Galileo (Europe), Beidou (China) and GLONASS (Russia). India (IRNS) and Japan (QZSS) also operate regional GNSS systems.

GPS (Global Positioning System) is the predominant GNSS system. Most aircraft systems documentation refers to "GPS" rather than "GNSS", and flight crew use "GPS" as standard terminology.

We therefore use the term "GPS" in this report.

Spoofing location terminology

Spoofing Location
Where an aircraft can expect to experience GPS Spoofing

Spoofed-to position
The false GPS coordinates received by the aircraft GPS receiver.

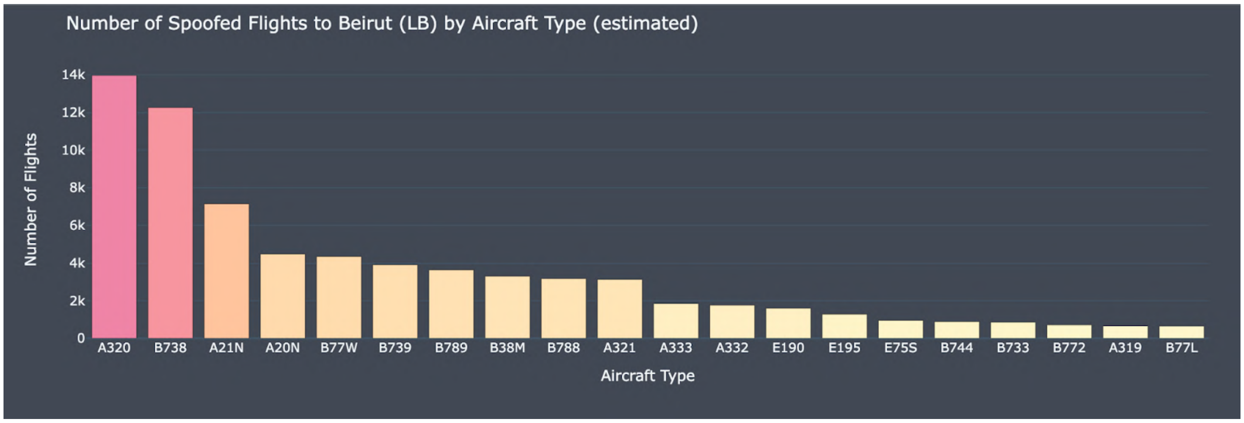
Spoofing Transmission Source
Where the Spoofing equipment is located. This may be a single transmitter or a network of transmitters. It's important to note the location of the spoofing transmission source is usually **not** the same as the spoofed-to position.

Aircraft Types affected

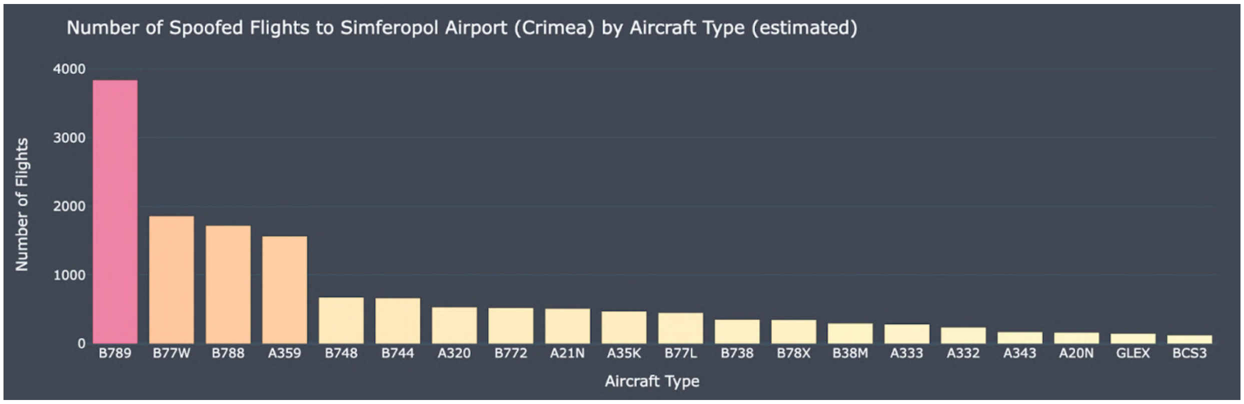
An analysis of the different aircraft types affected by GPS spoofing reveals that all GPS-equipped airframes are vulnerable to this threat.

The figures below show the **top fifteen** aircraft types affected during the period January - July 2024 in two example areas: the Black Sea and the Middle East.

In this data, the number of flights affected by type is more representative of the traffic types in the regions – the Eastern Mediterranean has far more short- and medium- haul traffic than the Black Sea region.



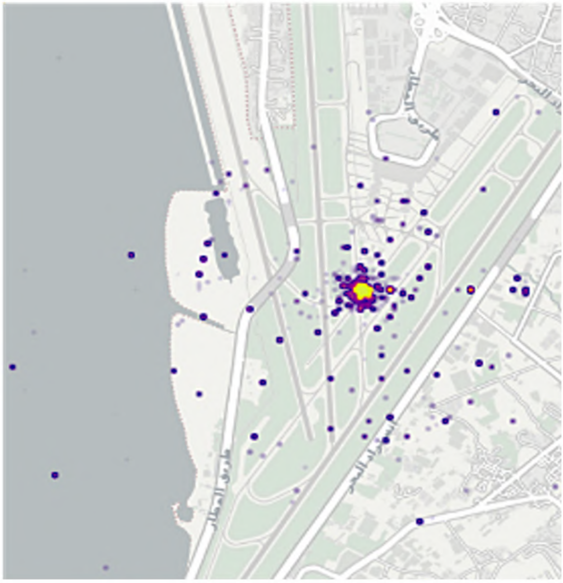
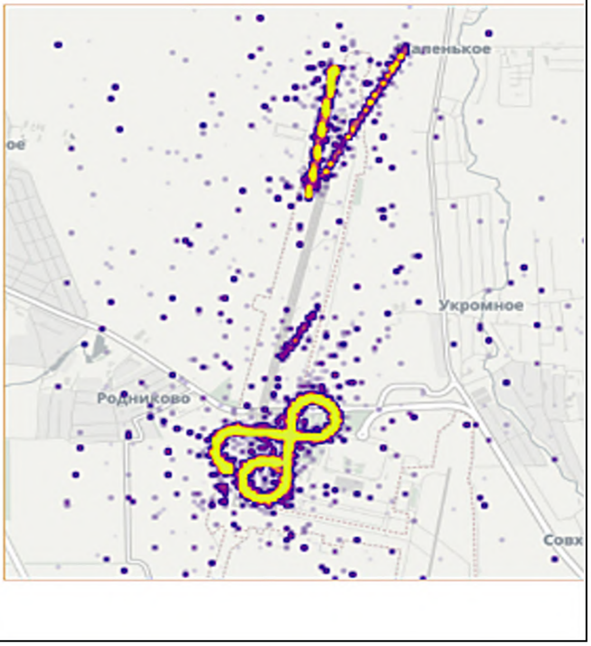
Top 15 aircraft types shown. Data source: ZHAW/SkAI.

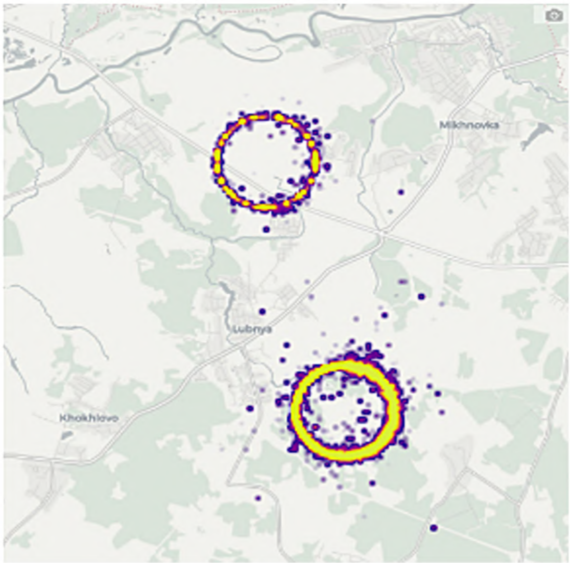
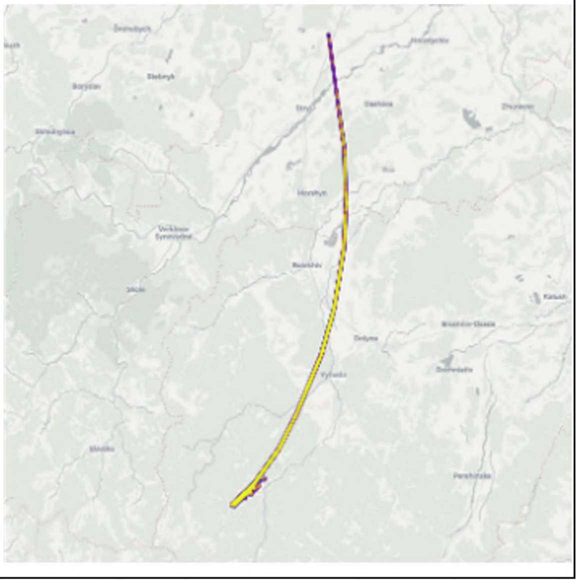


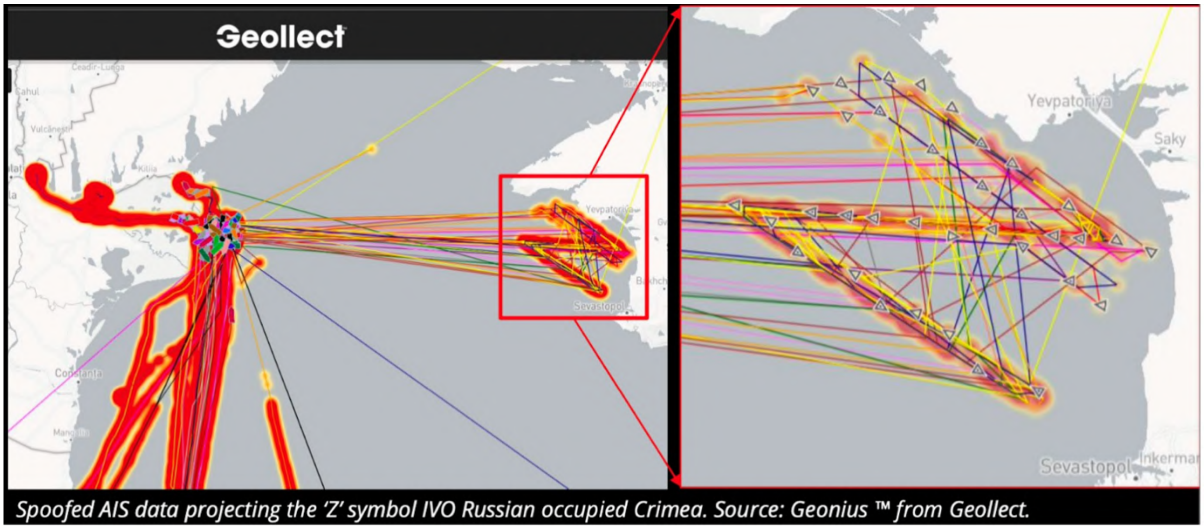
Top 15 aircraft types shown. Data source: ZHAW/SkAI.

Spoofing Patterns

The falsified GPS positions created by spoofers aren't always the same. In some cases, they are fixed in one place, but in other examples seen they move in circles, form complex patterns, or even mimic realistic paths.

Static Location at Beirut Airport:	Complex patterns at Simferopol
	

Circular Spoofing near Smolensk:	Along a realistic path in Ukraine:
	



Spoofed AIS data projecting the 'Z' symbol IVO Russian occupied Crimea. Source: Geonius ™ from Geollect.

Typical GPS Spoofing Equipment

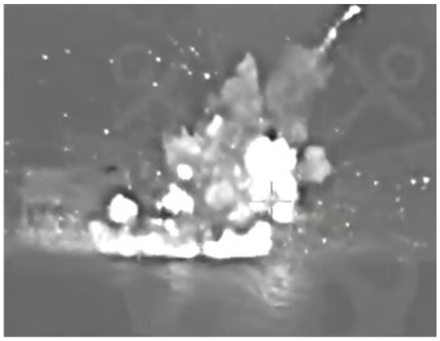
As noted above, almost all spoofing currently affecting civil aviation is being carried out by large-scale military Electronic Warfare equipment, by multiple countries. Examples of this type equipment are below.

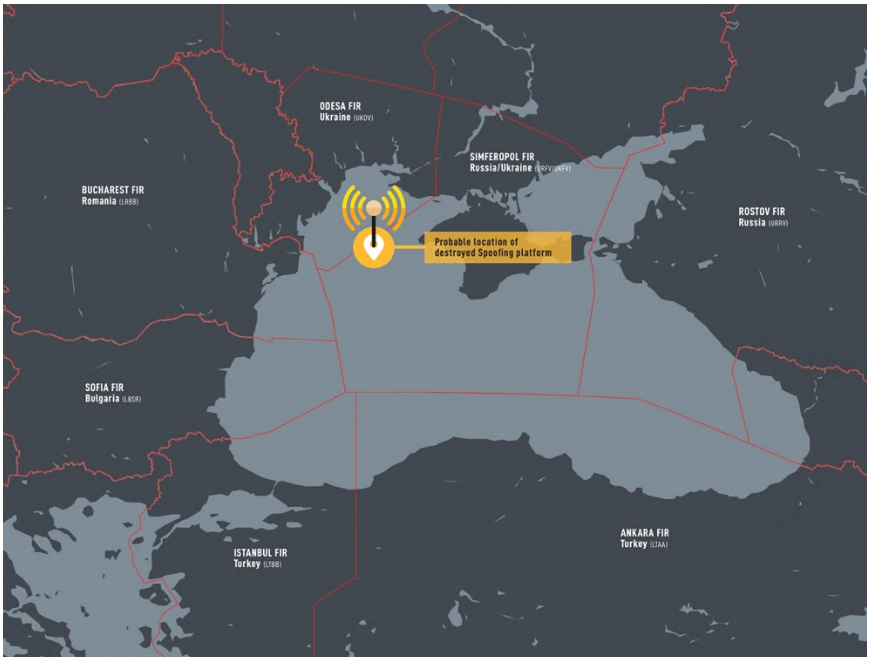
The R-330Zh Zhitel is a mobile truck-mounted electronic warfare (EW) station

The Krasukha is a mobile, ground-based, electronic warfare (EW) system

Oil Rig as GPS Spoofing Platform

In August 2024, a disused oil rig being used by Russian forces for GPS Spoofing was destroyed by Ukraine. As a result, spoofing levels in the Black Sea area reduced significantly, confirmed by data from SkAI and Spirent. The Ukrainian Navy said "[Russian forces] used this location for GPS spoofing to endanger civilian navigation. We cannot allow this". The target of the spoofing was on maritime vessels, but civilian aircraft receive the same spoofed signals.

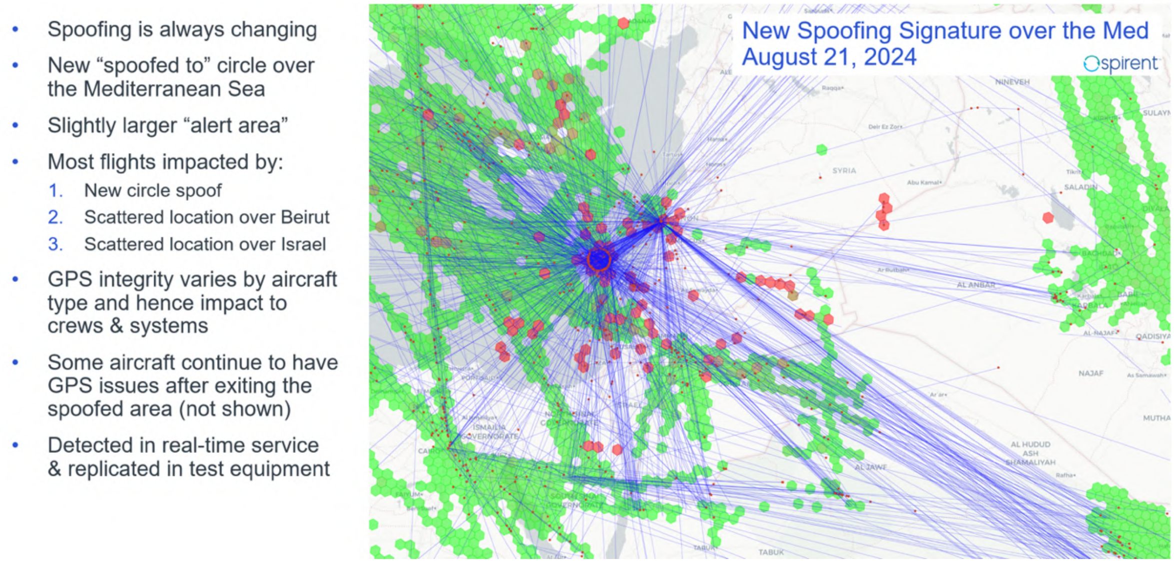




Changes in Spoofing Locations and Patterns

There is constant evolution in GPS Spoofing locations and patterns, with significant changes as often as weekly or even daily. This highlights the need for operators and crews to have access to a very current spoofing location map. Some examples of changes are below.

Changed spoofing pattern in the eastern Mediterranean, August 2024

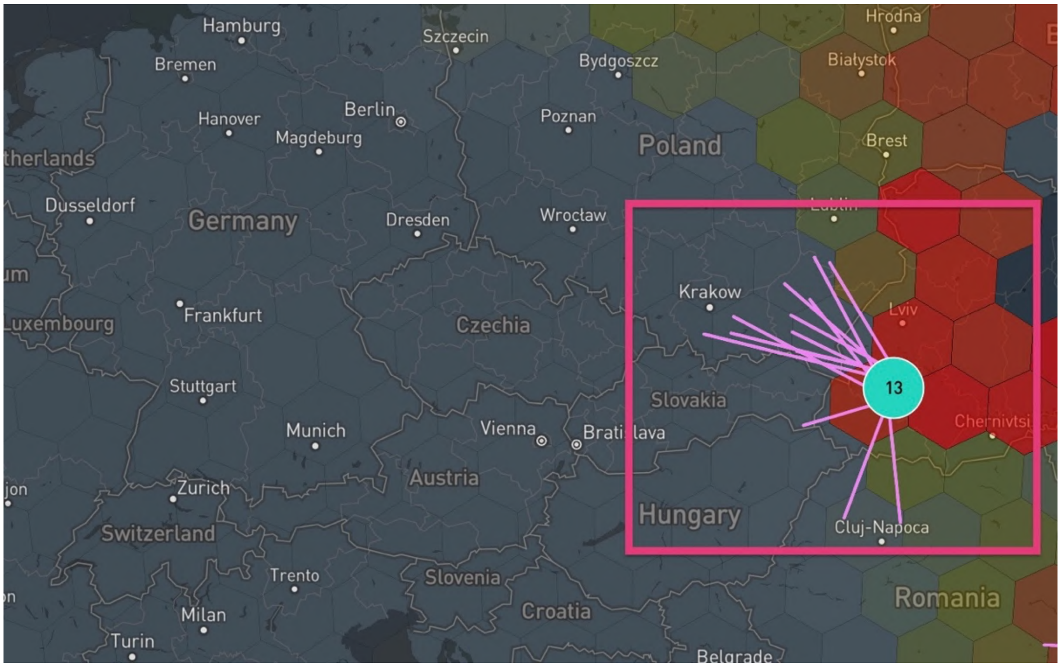


- Spoofing is always changing
- New "spoofed to" circle over the Mediterranean Sea
- Slightly larger "alert area"
- Most flights impacted by:
  1. New circle spoof
  2. Scattered location over Beirut
  3. Scattered location over Israel
- GPS integrity varies by aircraft type and hence impact to crews & systems
- Some aircraft continue to have GPS issues after exiting the spoofed area (not shown)
- Detected in real-time service & replicated in test equipment

New Spoofing Signature over the Med
August 21, 2024

spirent

New Spoofing location in western Ukraine, August 2024



Further Technical Information

Spoofing Tactics

- A spoofing technique employed by one “state actor” is to jam the secure GPS L2 frequency (1227.60 MHz), whose Precise Code (P-Code) is used by military systems to provide increased PNT performance, to force the use of the Civil Access (C/A) code on the L1 (1575.42 MHz) frequency. The state actor then spoofs the unsecured L1 signal. **It makes the spoofing easier**, because they only need to spoof one set of signals. The second civil frequency L5 signal (1176.45 MHz), which has not yet been incorporated in avionics GPS receivers and is not fully supported by the constellation, is stronger than L1 and will require higher powered jammers however, these are also emerging in some theatres of operation.

- At the moment, the dominant factors in a spoofer selecting constellations, frequencies, and codes to broadcast will be power budget and the most commonly used signals. Transmitting maximum power on only one frequency gives much greater jamming and spoofing range than transmitting that same maximum power over many more frequencies and signals. However, as receivers move to use more frequencies and signals, it will not be difficult for the spoofers to adjust. So, using more than one GNSS constellation and using more than one frequency (e.g., GPS L1 and L5) may provide a very short-term protection in some areas, but it **is not a long-term solution** to the problem beyond the time taken for the spoofers to change some settings in their menus on their spoofing devices.

Code phase

The time delay for a GPS satellite signal to travel from the satellite to the receiver provides the measure of the distance between the satellite and the receiver. However, this distance measurement is impacted by delays that occur as the signal passes through the ionosphere. Augmentation systems, such as WAAS and EGNOS provide data to allow these errors in distance measurements to be removed. The code phase of the received signal is a measure for this distance and refers to what section of a given satellite's coded broadcast is arriving at a particular moment in time. The code phase is estimated by matching the satellite's unique Pseudo Random Number (PRN) code with a local copy of this code. If there is a match, then the receiver has detected the signal (see acquisition above). These codes are 1 millisecond long for GPS C/A and 4 milliseconds long for Galileo E1, and due to the speed of light these codes effectively each span a distance of 300 km long and 1200 km long respectively from end to end when broadcast. By measuring the code phase accurately to a few nanoseconds, the receiver can calculate the distance to the satellite to an accuracy of a few meters. The carrier phase can also be measured to determine the distance between satellite and receiver to an accuracy of centimeters.

Navigation data

The navigation data contain various parameters that are used during the operation of the receiver such as satellite orbital parameters and clock corrections. Also, the navigation data provide an indication of the GPS satellites' health. If the spoofer broadcasts incorrect navigation data (which is generally the case), then the GNSS receiver may continue to calculate incorrect results even after it leaves the spoofing area and receives the true ranging signals again. This will continue to be the case until the receiver is manually reset or the navigation data "expires" and is refreshed automatically (which may never happen if the spoofer broadcasts its data such that the spoofed navigation data expiration date has been set to some time well in the future).

Doppler shift

GPS satellites orbit approximately 20,200 km above the Earth in what is called Medium Earth Orbit (MEO) and travel with great speed relative to receivers. This speed relative to the receiver results in a Doppler shift in the received signal compared to a situation where both the transmitter and the receiver are static. The Doppler shift measurements are used in both the position and velocity calculations for the receiver. Monitoring abnormal Doppler measurements compared to other sources of velocity on the aircraft provides receiver manufacturers with a valuable indicator of potential spoofing attacks.

RAIM

GPS receivers have Receiver Autonomous Integrity Monitoring (RAIM) algorithms to detect and mitigate erroneous GPS signals. These algorithms offer some protection against errors from a faulty satellite broadcast. For example, RAIM detects spoofing where the receiver tracks both real and fake satellite signals that cause inconsistent measurement data if only one or a very small number of signals are affected by spoofing and the vast majority are not. The RAIM Horizontal Integrity Limit (HIL) must be valid before the GPS output is used by airplane systems.

Traditional RAIM algorithms protect against a single faulty satellite by trying all "leave one out" PVT solution calculations. If one position fix is clearly different from the rest with much lower residual errors on each signal going into that fix it reveals the presence of a single faulty satellite. The computational load increase of moving from 1 faulty satellite to N faulty satellites is exponential. **RAIM was never designed to protect against spoofing and is not able to detect a case where all the signals are spoofed and would thus all deliver consistent information**.

Concern of corrupted GPS receiver appearing normal

Due to the way GPS receivers are designed, the only way to ensure that a GPS receiver will be trustable after any exposure at all to a spoofing attack is to fully reset the internal states of the receiver, by power cycling it, or by sending a "cold restart" command in software. There are even examples of some receivers that have been so disrupted that a full factory reset by returning the device to the manufacturer has been required.

This is true even if the receiver "**appears to have recovered**" after leaving a spoofing region. It is in fact still possible for the receiver to output false information later on in the flight, even hours later. For the interested reader, a full explanation of this is given here.

The orbital data for each satellite is continually broadcast by each satellite, and the receiver downloads the orbital data from each satellite regularly. This data is called the *ephemeris*. It takes about 20 -30 seconds to download it and each satellite only broadcasts their own. The ephemeris contains within it a timestamp which acts as an "expiry time" for that dataset. If the current time is too long after the expiry time the receiver will typically refuse to use that orbital data and will wait for fresh ephemeris to be downloaded.

If you have incorrect ephemeris data (e.g., a corrupted download, or because of a spoofing attack), you can't calculate the correct distance to the satellite when receiving its timing data. The following worst-case scenario addresses the case where a receiver continues to output corrupted measurements many hours after leaving a spoofing area.

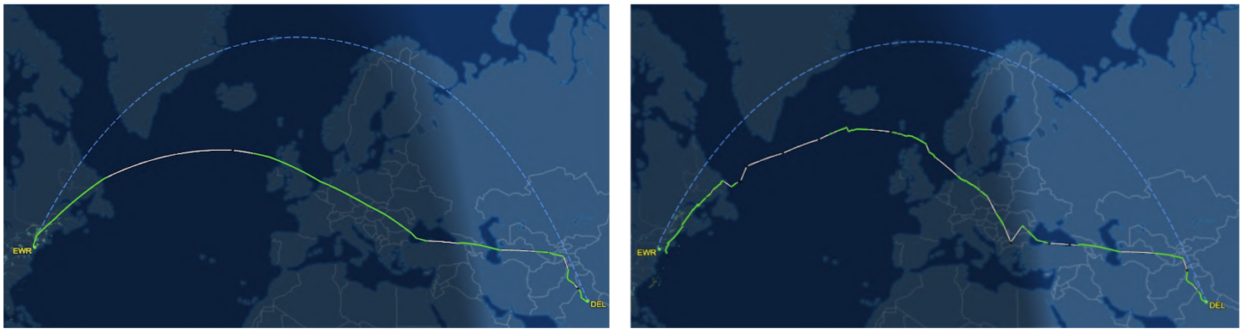
In this scenario, consider a receiver that is initially working correctly and is tracking the GPS satellites numbered 1, 2, 3, ….8, 9, 10 that are currently above the horizon. The other satellites are currently below the horizon. The receiver now flies into a jamming and spoofing zone. The receiver loses the lock of the satellites in the sky. The spoofer is broadcasting satellites 13, 14, 15, …, 19, 20 and so the receiver locks onto and downloads all of those ephemerides (from the spoofer's signals not from the real satellites). The spoofer is also transmitting the time a few hours into the future (we regularly see spoofed times and dates set to the future in the current interference regions). The receiver is then spoofed and reports incorrect positions, velocities, and times. The pilot ignores the data and flies through the spoofing region. The spoofed signals for satellites 13 to 20 fade away, as does the jamming signal, and the receiver picks up the signals from the real sky again, i.e., satellites 1,2, 3….to 10. The position fixes and time all now look correct, and it may reasonably be assumed that the receiver has recovered. However, this is not the case at all, as will now be explained.

As the aircraft continues its planned flight and an hour or more passes, the satellites visible in the sky start to change. Some of the satellites in the set 1, 2, 3…10 pass over the horizon and some of the real satellites from the spoofed set 14 to 20 are now rising in the sky. The receiver locks onto them and decodes the timing data and ephemerides from the real satellites. However, the corresponding time of applicability for the spoofed data has remained in the receiver's memory, and the key time stamp is still an hour later in time than the one being broadcast by the real satellites in the sky. As a result, the critical software code inside the receiver that checks these timestamps does not trigger the replacement of the spoofed orbital data with the real data. This will only occur at some point in the future when enough time has passed for the "expiry time" for the spoofed ephemeris data to finally be at some point in the past, rather than still being in the future. So, now the problems begin:

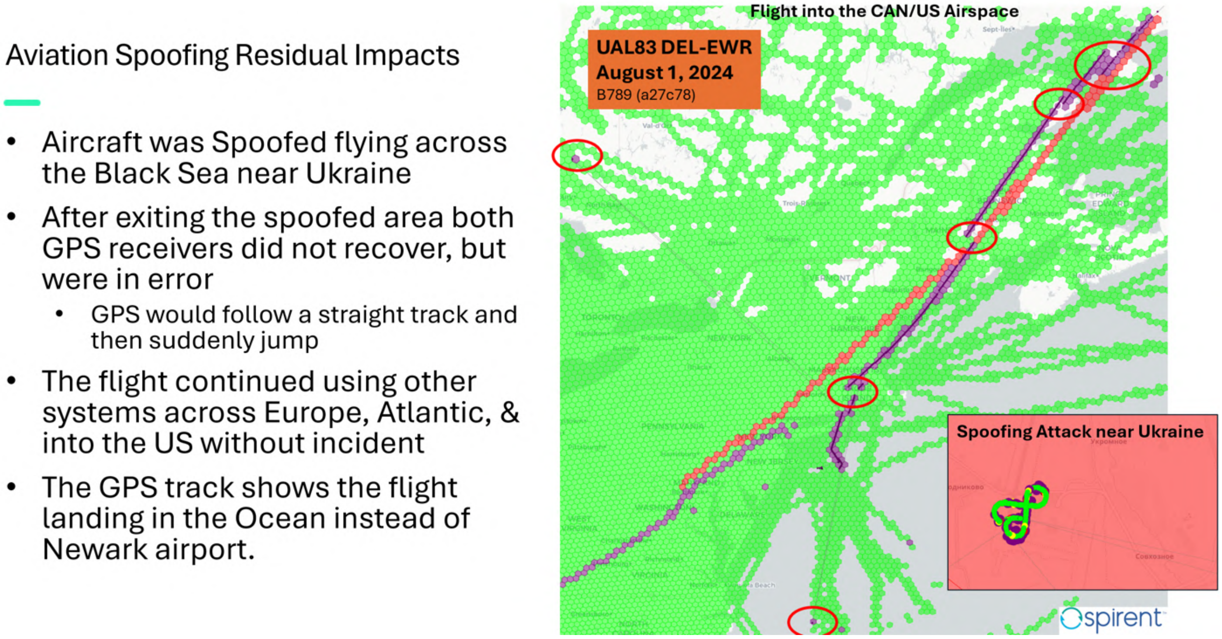
The receiver now tries to use the real satellite measurements with the incorrect spoofed orbital data still stored in its memory. The result is that there are nonsensical calculations and large discrepancies among the satellite measurements. Using an approach called "Receiver Autonomous Integrity Monitoring (RAIM)" the receiver attempts to detect and ignore a single "broken" satellite. The navigation system's Kalman Filter also provides another layer of protection against a small number of erroneous satellite measurements. However, as time passes further and satellites keep rising and setting, eventually very few usable satellites are visible and the majority of the authentic GPS signals are coming from the set 14 to 20, with incorrect orbital data. By now the receiver is outputting unusable and erroneous data and it is likely that its performance will have further degraded as the "good" satellites disappear one-by-one below the horizon. Although the time will be correct, the positioning has gotten worse and worse over time. The best-case scenario now is for the receiver to cold restart itself, but most will not do this. They will instead do a "warm restart", which means reacquiring the satellites and restarting the Kalman Filter, but critically not wiping all of the orbital data from memory.

While this scenario might not occur after every spoofing event, it is a plausible scenario and evidence exists that such scenarios may indeed be playing out. The image below shows UAL83's 22 May 2024 and 1 August 2024 flight from Delhi, India (VIDP) to Newark, USA (KEWR). While the May flight path is as expected, the August flight exhibits a highly unusual tracking solution, which neither conforms to the expected flight path nor looks like a coasting inertial reference system (which would show a smooth divergence over time without jagged resets and jumps). Nor does it look like a functioning GNSS receiver. The behavior that it does exhibit can be explained by a GPS receiver that keeps resetting its navigation Kalman Filter, but is forced to keep calculating fixes using a mixture of valid and invalid measurements.

Different receivers may have different logic and thresholds for how and when to refresh the orbital data for all satellites, and so the scenario above should be discussed with GPS receiver providers to understand under exactly what scenarios a receiver would and would not replace the current orbital data with new data being decoded from the satellites.



These figures show UAL83 DEL-EWR flights on 22 May 2024 (left) and 1 August 2024 (right). The journey on the left seems to be an example of the expected route for this journey. The journey on the right exhibits significant and sustained disruption to the tracking performance for the entire flight, following an exposure to GPS spoofing early on in the flight.



Aviation Spoofing Residual Impacts

- Aircraft was Spoofed flying across the Black Sea near Ukraine
- After exiting the spoofed area both GPS receivers did not recover, but were in error
  - GPS would follow a straight track and then suddenly jump
- The flight continued using other systems across Europe, Atlantic, & into the US without incident
- The GPS track shows the flight landing in the Ocean instead of Newark airport.

Flight into the CAN/US Airspace

UAL83 DEL-EWR
August 1, 2024
B789 (a27c78)

Spoofing Attack near Ukraine

Further analysis of the same flight, UAL83, on August 1, 2024. Source: Spirent.

GPS Spoofing

Impacts

This section assesses the **impact** of GPS spoofing on:

- Aircraft Handling
- Aircraft Operation
- Air Traffic Control

This is followed by a brief technical description of how GPS spoofing affects individual aircraft systems.

GPS Spoofing Impact Matrix

Spoofing effect	Aircraft Handling Flight Crew	ANSP/ATC Air Traffic Controller	Operational Aircraft Operator
GPS receiver failure	*Impacts other systems* - May appear recovered but still contaminated		- AOG if receiver becomes 'bricked' (NVM corrupted) - Repair time days or weeks COST
FMS position degraded or failed	- Undetected off-track navigation - Loss of situational awareness - Unplanned entry into Danger Area, other FIR's	- Lateral loss of separation - Vectoring (often many aircraft) - increased workload	- Potential Accident/Incident RISK
Unable RNP	- Restricted to conventional enroute navigation and approaches - Unable RNP SID/STAR - Reduced Oxygen Escape route options	- RNP-4 or better based separation not available e.g., North Atlantic - RNP App/SID/STAR not useable - Increased vectoring for initial approach	- Potential diversion COST
Map Shift	- Wrong runway selection - Loss of situational awareness	- Loss of separation during landing - Risk of landing on closed runway	- Potential Accident/Incident RISK
IRS	- Hybrid IRS may cause false FMS position or failure		
GPWS	- False EGPWS alerts - Startle effect - Lowered trust in GPWS system overall - Delayed responses - Go-around from unusual altitude/position - Nuisance alerts cause stress, distraction - Risk of response in low-energy aircraft state, stall.	- Level busts, loss of separation due to unexpected EGPWS response maneuver.	- Potential Accident/Incident - Passenger injury RISK
Weather Radar	- May impact ability to detect Cb - Ground clutter function not available		- Potential flight into convective activity - Passenger injury RISK
Aircraft Clock	- Incorrect time displayed on clock - Incorrect time fed to other systems		

Spoofing effect	**Aircraft Handling** Flight Crew	**ANSP/ATC** Air Traffic Controller	**Operational** Aircraft Operator
Datalink (ADS-C, CPDLC)	- CPDLC not available, switch to voice (VHF, HF) - ADS-C not available - Oceanic RCP/RSP cannot be met, PBCS tracks not avail - Reroutes or lower levels can be expected	- European capacity constraints due to overuse of VHF - Oceanic PBCS separation not available	- Reroute - Diversion - Lower level, higher fuel burn COST
ADS-B	- Unable to fly in ADS-B required airspace	- ADS-B only airspace not available - ADS-B based separation not available - Risk of incorrect ADS-B based position on screen	- Reroute - Cancellation COST
HUD & SVS (Synthetic Vision)	- HUD must be stowed - SVS not available - Degraded situational awareness		
ELT	- Potential for incorrect aircraft position broadcast in emergency	- SAR may receive incorrect aircraft position	- SAR in wrong location RISK
RAAS (Runway)	- Unavailable, or may give false warning		- Potential Accident/Incident RISK
ROPS (Runway)	- Unavailable, or may give false warning		- Potential Accident/Incident RISK
SATCOM	- May be unavailable		
EFB	- Some applications use GPS position and will not work correctly (e.g., moving map) - Situation awareness degraded		
Internet/Wi-Fi	- Some reports of Wi-Fi not working correctly		- Pax inconvenience
Overall: Complexity of multiple interconnected failures	- Complex go-arounds with multiple failures - Emergency margin of safety reduced		- Potential Accident/Incident RISK - Diversion COST

Analysis of impact of GPS Spoofing

The impact of GPS Spoofing - and Jamming - on aircraft systems, handling, and the wider flight operation, is complex. It is best divided into two areas:

1. **Unavailable GPS Receiver**: the impact of having **no** GPS information available.
2. **Contaminated GPS Receiver**: the impact of **false** GPS information.

Unavailable GPS Receiver

Both GPS Spoofing, and GPS Jamming, render the aircraft GPS receiver unusable. Whether in a failed state due to jamming, or a contaminated state due to spoofing, the receiver can be described as simply being "**not available**". This list only details the consequences of "no GPS signal", not the introduction of false information in spoofing.

1. GPS Not Available for Enroute Navigation

Limitation: Without a functioning GPS receiver, GPS based navigation is not possible.

Alternative: For enroute navigation, IRS and Radio Navigation have historically provided sufficient navigation accuracy for all enroute areas, including Oceanic and Remote regions.

2. GPS Not Available for Approach Navigation

Limitation: Without a functioning GPS receiver, GPS based approaches (such as RNP approaches) are not available.

Alternative: Conventional approaches (ILS, ILS/DME, VOR(/DME), NDB) are available, and remain operational at the vast majority of airports.

3. GPS Not Available for Aircraft Systems

The primary use of GPS is for aircraft navigation. However, as has become clear since GPS Spoofing began, it is also widely used in other aircraft systems.

Limitation: Without GPS, the following system components are not available:

- **EGPWS**. GPS is required for position and altitude to enable the enhanced portion of GPWS.

- **ADS-B.** GPS is the primary source of position information for the broadcast of aircraft position through ADS-B. Regulations and standards for ADS-B generally assume the availability and use of GPS signals for position broadcasting

- **Runway Overrun Protection Systems**. GPS is required for position information.

Alternative:

- **GPWS basic mode** (based on radio altimeter) with limited function and alert time.

- **Conventional surveillance** (Primary and Secondary Radar), Multilateration, ADS-C.

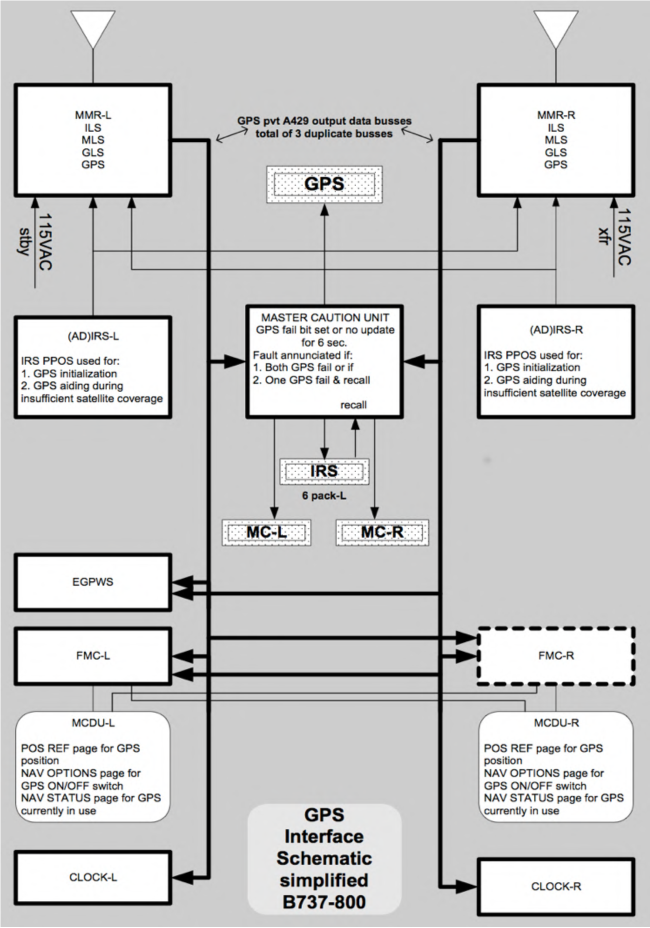
Thus, without GPS, the aircraft must be navigated using IRS or Radio Navigation. GPWS is restricted to basic modes only, and ADS-B and Runway protection systems are not available.

Contaminated GPS Receiver

In a GPS Spoofing encounter, the GPS receiver becomes contaminated with false information. This typically includes a false position (wrong coordinates), false date and time, false altitude, and often false system settings (e.g., Ephemerides, or table of satellite positions).

Once false GPS PVT data (Position, Velocity, Time) is passed by the GPS receiver **to other aircraft systems** via the ARINC 429 Data Bus (DITS), the list of impacts and failures becomes much longer than a pure loss of signal as outlined earlier.

What quickly becomes clear as a major issue, is the current inability to isolate the GPS receiver from other aircraft systems.



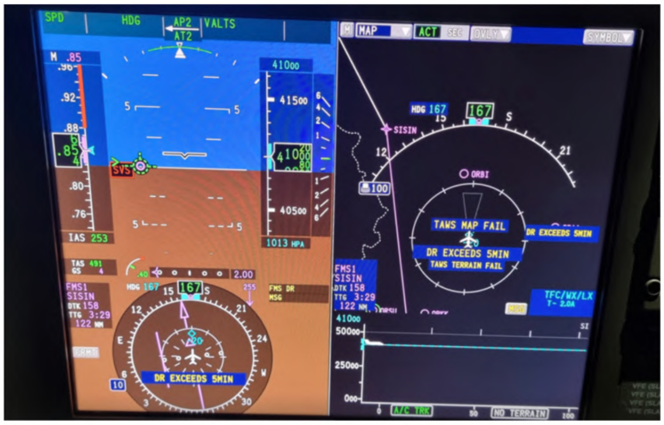
FMS position calculation

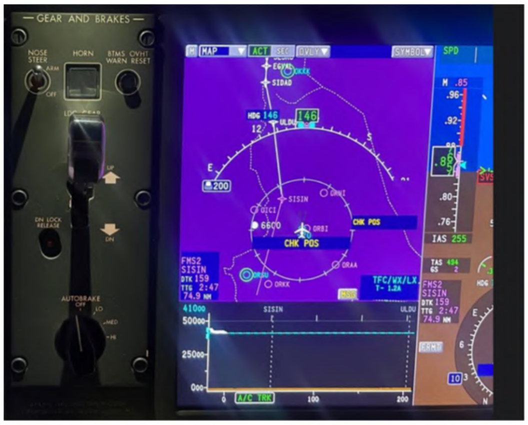
With false GPS position information, the FMS position can become corrupted. It **may not be immediately obvious to flight crew**, and the aircraft can subtly drift or turn off route.

In some aircraft, the FMS can quickly "fail-down" to Dead Reckoning, if the other systems have a GPS element. In DME/DME and VOR/DME updating, positions of the ground aids are stored in a database in the FMC. With a false GPS position, the DME/VOR aids will be rejected as being too distant. If the IRS has a GPS-Hybrid element, it too can fail.

The traditional sensor input linear hierarchy is: GPS, DME/DME, VOR/DME, IRS (if installed), Dead Reckoning. In more recent FMS systems, the hierarchy is modified to a non-linear, logical structure, essentially looking for the sensor with the highest accuracy. When spoofed, the GPS can report high integrity and be incorrectly chosen by the FMS. On systems with a Hybrid IRS input, this will be the sensor most commonly selected.

FMS position errors can also cause "**Map Shift**", i.e., the Navigation Display (ND) incorrectly showing the aircraft in a location other than its true position.





IRS

A traditional, **"Self-contained" IRS** does not receive GPS inputs, and so is not impacted by spoofing. The only threat vector is if the IRS is manually aligned on the ground in a spoofing location, using a GPS position that is spoofed.

The newer (~2010 onwards) **"Hybrid" IRS systems** are vulnerable to false GPS information during a spoofing encounter. Hybrid IRS systems provide greater accuracy but use the GPS data for updating position. Hybrid IRS systems calculate both a hybrid position and a "Pure-IRS" position. The "Pure-IRS" position solution is subject to normal drift but is not impacted by spoofing.

GPWS

GPWS Basic GPWS works by measuring the aircraft's height over the ground (and the rate of change of that height) through the use of radio altimeters. Basic GPWS combines the radio altitude of the aircraft together with the aircraft's configuration (flaps and landing gear) and instrumentation (ILS glide slope) to issue caution and warning callouts to the crew.

Basic GPWS is not impacted by GPS Spoofing.

EGPWS Enhanced GPWS works by overlaying the aircraft's computed position with a database of known runways, terrain and obstacles to create caution and warning envelopes ahead of the aircraft which will trigger the relevant callouts and warnings. Also referred to as "GPWS Look Ahead Terrain". Although the EGPWS can use IRS horizontal position information as a backup if GPS position is not available, it relies on GPS altitude to calculate "Geometric Altitude". During spoofing, this altitude information becomes corrupted, and leads to the false alerts later in flight.

Enhanced GPWS is severely impacted by GPS Spoofing.

Weather Radar

Some commonly used weather radars use GPS position to assist with "Ground De-cluttering". GPS information is taken from the EGPWS, rather than directly from the GPS receiver.

Crews report unusual weather radar behavior after spoofing, including inability to detect Cb cells (Thunderstorms). Weather radar issues may also present due to RF interference around spoofing areas, rather than directly from GPS spoofing.

Aircraft Clock

The aircraft clock is constantly updated in-flight by the time/date portion of the GPS Signal. During spoofing, the time has been noted to change to an incorrect time, including a date and time in the past, or well into the future.

This renders the aircraft clock unserviceable, but of greater impact is the flow-on effect to datalink systems, discussed next.

Datalink: CPDLC and ADS-C

CPDLC and ADS-C use a timestamp taken from the aircraft clock. **If this time is corrupted by spoofing, CPDLC and ADS-C may be lost.**

There are differences between how the ATN and FANS systems will respond to a time error:

ATN (Aeronautical Telecommunication Network) logon reports the time and date. With an incorrect time or date, ATN data link messages can be rejected by the ground system perceived as too old in the past or as in the future. If the aircraft is already logged on to ATN when the time or date becomes incorrect, any subsequent uplinks show "INVALID UPLINK" (not visible to crew) due to the difference in time and date between the aircraft and ground system. The ground system can disconnect from the aircraft due to the error in which case the ATN connection will be terminated and indicated in the message "ATC COMM TERMINATED".

FANS (Future Air Navigation System) do not compare date or time between the aircraft and ground systems. Current airplane time is appended to any FANS CPDLC uplinks, but all FANS CPDLC functionality remains the same if time and date are incorrect. However, if a FANS CPDLC Uplink Delay Monitor is established between ATC and the airplane, uplinks appear to be old due to the incorrect airplane time or date. The resulting text "UPLINK DELAY EXCEEDED" is shown on the uplink message header. However, the flight crew can still respond to this message and utilize FANS CPDLC normally.

The position information inserted in ADS-C reports will have a downgraded accuracy. The downgrading will be detectable by controllers, via a specific field of the ADS-C report called Figure of Merit (FoM) set to a specific value (30 nm) in order to inform of the GPS loss. ADS-C uses FMS position rather than GPS position.

Spoofing can therefore result in loss of datalink.

ADS-B

ADS-B Out

ADS-B relies completely on GPS position to broadcast the aircraft position. It does not take inputs from alternative navigation systems that may be available on the aircraft.

A false ADS-B position may be broadcast. In this case, ATC may observe a position difference between ADS-B Out position and airplane position on primary and secondary radar.

ADS-B in

ADS-B In traffic is removed from the ND. TCAS traffic shows. ADS-B only traffic may be shown at an incorrect position on ND, caused by reception of incorrect ADS-B OUT data. Long range ADS-B IN targets that are outside of the TCAS validation range (40 nm around own-ship) can be displayed in incorrect locations or be missing from ND depending on the severity of spoofing. Normal TCAS functions are not affected for the traffic inside the TCAS validation range.

Radio Navaid Tuning

Automatic tuning of Navaids by the FMS is degraded or not available after spoofing. This is due to the FMS using a table of nearby navaids for auto-tuning based on present aircraft location. If the FMS GPS position downgrades due to GPS Spoofing, automatic selection of VOR, DME, etc. will not be possible, further complicating the navigation solution.

Head Up Display

In jamming events, prolonged GPS signal loss can cause lateral displacement of the FPV of up to two degrees. Spoofing can affect some displayed HUD functions, identified by lateral misalignment of HUD FPV and runway depiction.

Runway Awareness and Advisory System (RAAS)

On airplanes equipped with RAAS, when the GPS signal is lost, RAAS is unavailable and either RUNWAY SYS or RUNWAY POS are shown on EICAS. RUNWAY SYS is displayed for complete loss of GPS signal. RUNWAY POS is only displayed if GPS is not accurate enough to support the function (i.e., horizontal figure of merit exceeds 0.02nm). Jamming would most likely lead to the former. Spoofing could lead to the latter. Ground proximity alerts that occur are valid.

Runway Overrun Prevention System (ROPS)

The Runway Overrun Prevention System (ROPS) is made up of two sub-functions: runway overrun warning (ROW) and runway overrun protection (ROP). The ROW function generates alerts which incite the flight crew to perform a Go-Around whereas the ROP function generates alerts which incite the flight crew to apply available deceleration means.

Emergency Locator Transmitter (ELT)

Modern ELT's use GPS position to transmit distress on 406 MHz, which is intended to be picked up by satellite.

However, the GPS position here **comes from a receiver within the ELT itself**, and not the aircraft GPS receiver. Monitoring is conducted by the International Cospas-Sarsat Program. There are two ways they determine the user's position.

1. The user's GPS location is transmitted within the emergency distress signal (GPS receiver inside of the emergency beacon) and

2. Cospas-Sarsat exploits time- and frequency-of-arrival between their satellites to determine the user's location, which is independent of the contents of the message in 1.

Under normal operation, the positions in 1. and 2. match. During 2024, there were a number of cases where the GPS location transmitted by the ELT was actually a spoofed location, but the position information from 2. above could be used to determine real position.

There is potential for incorrect ELT position information due to spoofing.

Air Traffic Control Impact

There was a strong focus on assessing the impact of GPS Spoofing on Air Traffic Control (ATC) operations during the WorkGroup.

Just as for flight crew, there are a wide array of impacts to consider from the ATC perspective.

There are two distinct ways spoofing affects ATC:

- In-Sector Spoofing
- Downroute Sectors

In-Sector Spoofing

In-Sector Spoofing applies to an ATC sector where aircraft experience GPS Spoofing.

Several ATC units within Spoofing regions participated actively in the WorkGroup. For these ATC centers, Spoofing has become a daily issue. The following points were raised by the ANSP's/CAA's involved:

- Dramatic rise in the need for radar vectoring during and after spoofing. In one ATC Center, 382 aircraft were recorded as requesting vectors, out of 2,021 GPS interference reports.

- Radar vectoring places aircraft navigation responsibility onto the Air Traffic Controller, adding to workload and reducing overall scan ability, especially if multiple aircraft are requiring vectors simultaneously.

- Aircraft departing Spoofing affected airports (for example LCLK, LLBG, OLBA) were regularly observed tracking incorrectly on the SID, sometimes towards danger or restricted areas. Crew were often unaware. This adds challenge to providing separation, and requires greatly increased vigilance by the controller.

- Responses to (false) EGPWS alerts have caused uncoordinated climbs to unknown altitudes/levels, and loss of separation.

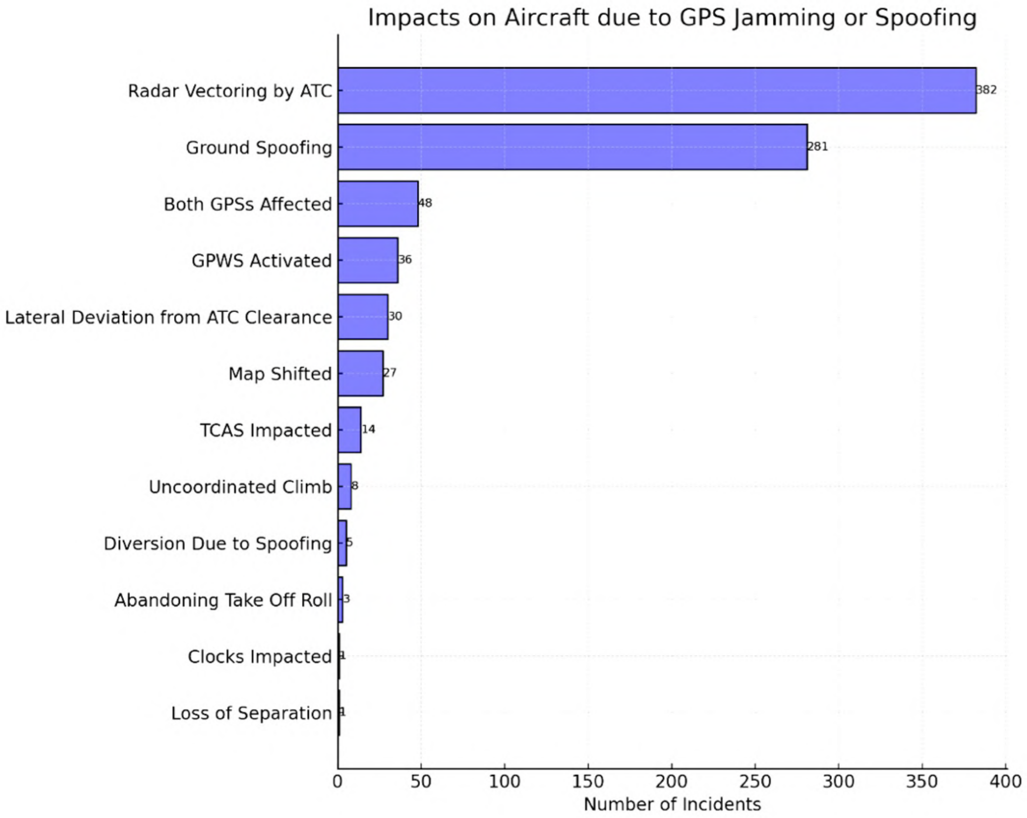
- Increased coordination with adjacent sectors was required to handle wayward tracking and unexpected climbs, increasing workload.

- Go-Arounds due to spoofing impact on aircraft systems have become common.

Case Study: Statistics for GPS Jamming/Spoofing impact

One ATC Center (de-identified) provided a summary of reports filed by controllers over a seven-month period:

- Data period is January 1st to July 31st, 2024. A total of 2,021 GPS Jamming and Spoofing reports were received. Only reported occurrences are included, the actual numbers are likely higher.
- 595 reports out of the 2021 occurrences have been classified as GPS Spoofing.
- 382 aircraft out of the 2021 occurrences required radar vectors due to inability to self-navigate.
- 281 aircraft were affected by "on-ground Spoofing"
- 36 reports of EGPWS activation, 14 reports of TCAS problems, 8 reports of uncoordinated climb (a "level bust"), all due to GPS Spoofing



Most affected Flight Information Regions

The FIR's most affected by in-sector spoofing during a one-month snapshot (July 15-August 15, 2024) were:

1. **Nicosia FIR, Cyprus** (5,655 flights spoofed)
2. **Tel Aviv FIR, Israel** (3,228 flights spoofed)
3. **Cairo FIR, Egypt** (2,375 flights spoofed)
4. **Ankara FIR, Turkey** (1,195 flights spoofed)
5. **Samara FIR, Russia** (1,186 flights spoofed)
6. **Moscow FIR, Russia** (988 flights spoofed)
7. **Lahore FIR, Pakistan** (492 flights spoofed)
8. **Minsk FIR, Belarus** (372 flights spoofed)
9. **Beirut FIR, Lebanon** (371 flights spoofed)
10. **Delhi FIR, India** (316 flights spoofed)
11. **Sofia FIR, Bulgaria** (235 flights spoofed)
12. **Bucharest FIR, Romania** (231 flights spoofed)

The actual number for some sectors is likely a lot higher, as the spoofing location can only be determined if a sustained period of jamming does not take place beforehand. Nonetheless, it gives a good indication of where most spoofing is taking place. The data is from SkAI Data Services, based on ADS-B data.

Downroute sectors

The challenges for ATC sectors downroute of spoofing regions are different, but equally challenging.

Navigation Capability

- A significant number of aircraft are left without GPS sensor input to the FMS after encountering spoofing. This results in "No RNP", or an inability to navigate other than by conventional means (VOR, DME, NDB) or using IRS inputs.

- For the North Atlantic, this regularly means that spoofed flights enter the NAT HLA without RNP-4 capability. RNP-4 is critical to capacity and safe and efficient traffic flows. Many aircraft are only capable of RNP-10. This impacts separation for NAT region controllers, and if delayed notice is provided by crew, can create last-minute re-shuffling of traffic and lower levels for the aircraft involved.

- Due to GPS Spoofing, specific forms of separation are not available to ATC:
    - PBCS separation (5 minutes longitudinal and 23 NM lateral)
    - 15 NM Target to target surveillance separation (based on RCP240 and surveillance)
    - 5 NM surveillance (in ADS-B only areas).

  This often has the effect that aircraft with reduced capabilities are descended to a lower flight level.

- An increase in GPS failures, from 1% of all traffic in January 2024, to 3% of all traffic in June 2024, was noted by one Oceanic sector.

Datalink

- CPDLC and ADS-C failures are common after GPS Spoofing. This is caused by a timestamp mismatch, as the aircraft clock time is changed during spoofing.

- Aircraft without CPDLC must revert to VHF or other voice means, which reduces sector capacity. This was regularly noted by European ATC Centers during the Workgroup.

- CPDLC and ADS-C failure has the same impact as lack of RNP-4 on the North Atlantic, as they are required elements for PBCS Tracks.

Safety Concerns

A list of ATC specific safety concerns is detailed in the Safety Concerns chapter. These include:

- Level busts & loss of separation
- Lateral deviation
- Increase in ATC workload
- Sector overload
- Surprise Climbs

The issue of "**Surprise Climbs**" was discussed in the Workgroup, and there was consensus that this required greater awareness and training. There are now regular occurrences of unanticipated EGPWS responses, at altitudes and positions not normally seen. This means that especially on approach, any aircraft could suddenly commence a high-energy climb. Traffic above is not protected in the same way that it might be when above a missed approach area, for example. Further, in the event of a surprise EGPWS response, TCAS RA inhibition during EGPWS response limits the conflict resolution dialogue between concerned aircraft.

Other ATC impacts / considerations

- A review of the roadway to PBN-only airspace is required, detailed in the Recommendations section.

- A major "open item" relates to the use of GPS in any way after a GPS Spoofing encounter. As detailed in the Technical section, a GPS receiver may **appear recovered, but in reality still be contaminated by spoofed values**. This means that RNP approaches, and RNP as used in enroute operations (e.g., RNP-4 on the North Atlantic) may not be assured as reliable after a spoofing encounter. See Technical section, UAL83 case study.

- Navaid inspection in Spoofing areas may be at risk, if GPS is used to verify the accuracy of Ground Based Navaids.

- Clarity was sought by Flight Crew regarding ability to enter Datalink Mandate domestic airspace (e.g., Europe) after a GPS Spoofing Encounter. A NOTAM to confirm that "Datalink Mandate may be disregarded after GNSS Interference", etc. would be helpful to alleviate crew concerns that they may be excluded from certain airspace.

- The creation of **standard phraseology** for GPS Spoofing reports, GPS failure notification to subsequent sectors, and most importantly EGPWS responses was considered important to address.

- NOTAMs regarding GPS interference (Spoofing/Jamming) were noted to be inadequate, and could better detail the locations (airways, positions) that spoofing is being encountered, as well as procedures to report interference to ATC.

Safety Concerns

These are the major safety concerns relating to GPS Spoofing.

The workgroup is **extremely concerned** about the overall impact of GPS Spoofing on flight safety. A total of **8 overall** safety concerns and a further **33 specific** concerns were raised.

These concerns are based on ATC reports, airline and aircraft operator reports, individual crew safety reports, the Workgroup survey responses, and analysis from Workgroup participants.

Overall Safety Concerns

This section details the **eight high-level concerns** that the Workgroup established, as a result of the GPS Spoofing problem.

Following this section, **specific safety concerns** will be listed for the following areas:

- **Aircraft operation and handling** (11 concerns)
- **EGPWS** (8 concerns)
- **Procedures and training** (4 concerns)
- **Human factors and CRM** (6 concerns)
- **Air Traffic Control** (4 concerns)

01 Dramatic increase in spoofing levels

GPS Spoofing, as currently being experienced by civil aviation, is a new phenomenon that has been happening for a little over 11 months. The number of flights affected has risen dramatically since May 2024. In a **one-month period** from July 15 to August 15, 2024, a total of **41,000 flights were spoofed**. The intensity of spoofing has increased, and the impacts are more severe. The large number of aircraft systems affected, and the complexity of multiple concurrent failures introduce a new operating environment that has not been risk-assessed. The greatest danger is what we don't know yet, but **may only come to learn through serious incidents or accidents**.

02 Winter increases operating risk

In this current phase of the GPS Spoofing problem a **500% increase** in spoofing has been observed. On average 1500 flights per day are now spoofed, versus 300 in Q1/Q2 of 2024. This is coincident with the summer months in spoofing affected areas. **With winter approaching, the operating environment changes from predominantly good weather and VMC conditions, to poor weather, icing, and IMC conditions.** This change will increase the risk factors significantly.

03 Risk of complacency

The Workgroup noted what presents as an **overall sense of complacency and muted interest** across a broad section of the aviation industry. This sense manifests through the sluggish initial response to the GPS Spoofing problem, the incomplete and delayed guidance to crews, and the lack of industry discussion on the latent and acute safety concerns, especially GPWS impacts.

In contrast, this largely pilot-led Workgroup has a high level of safety concern, and the survey of Flight Crew as part of the Workgroup research, showed that of the 1,997 respondents, a full 1,400 crew members (~70%) rated their **concern on flight safety impact**, as **very high or extreme**. 91% of all crew members rated their concern as moderate or higher.

04 GPS Complexity in aircraft systems

The high dependency on GPS, interwoven into at least 16 essential different aircraft systems, creates a **chain of complexity** that makes safety and risk assessment challenging, yet essential. Equally, the complexity created for crew by the **myriad of possible combinations of failed systems**, is a serious concern.

05 Lack of technical information

For flight crew, the Workgroup noted a **lack of availability of technical information on GPS involvement in aircraft systems**, conflicting crew guidance, and incomplete or insufficient procedures, all leading to misunderstandings and knowledge gaps. Common misconceptions evident in crew feedback include a common belief that de-selecting GPS inputs to the FMS “turn off” the GPS receiver itself, and that the EGPWS will be protected.

06 Crew forced to accept degraded aircraft

The large number of system failures during and after a GPS Spoofing encounter places the aircraft into a state where it **would not be possible to dispatch it before flight**, nor be acceptable to flight crew from a flight safety perspective. These include failures and issues with GPS Receivers, EGPWS, Weather radar, Primary navigation, FMS, IRS, CPDLC, ADS-B, ADS-C, Aircraft clock, RNP capability, TCAS (ADS-B in), Head Up Displays, and Runway protection systems, many of which persist long after the spoofing encounter.

In essence, **GPS Spoofing puts the aircraft into a significantly degraded state** which no pilot in command would accept before flight. Yet, crew are forced to accept that with great probability, the aircraft will become degraded in these ways during flight.

07 Potential for worsening of situation

To date, no aircraft has been directly targeted. However, the vulnerabilities identified in spoofing encounters so far mean that were this to change, the impacts could be even more severe.

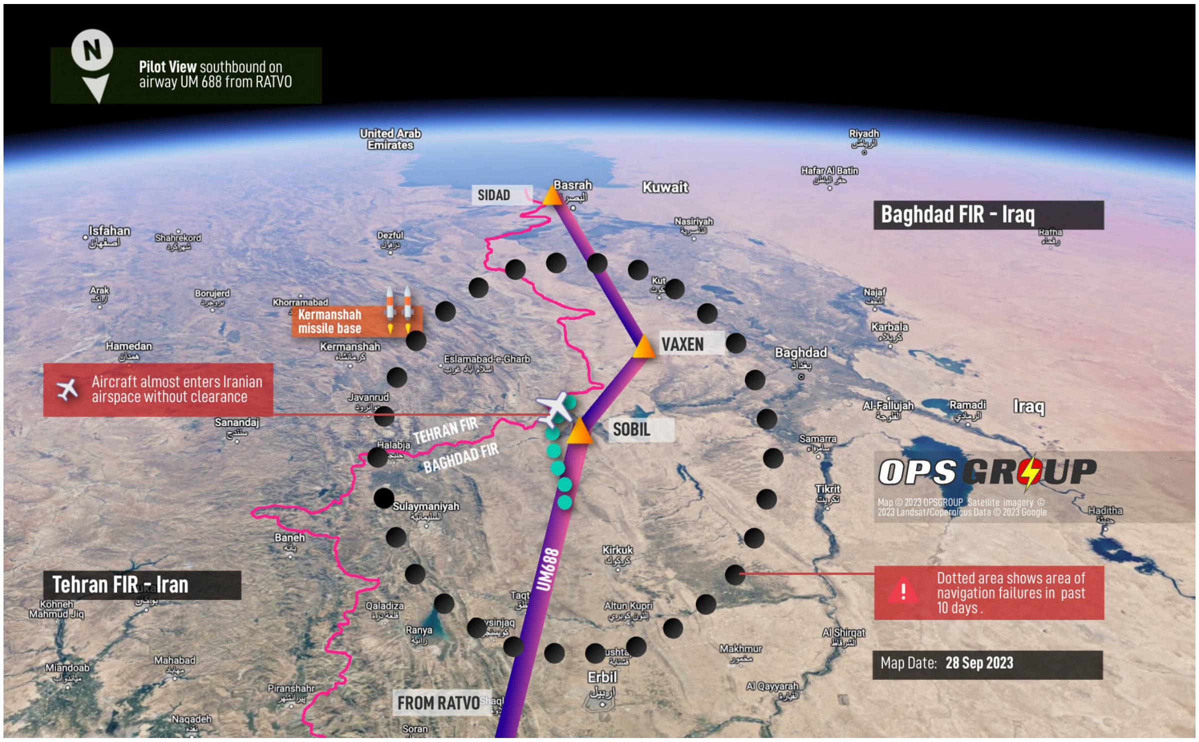
Even without direct targeting, the locations and spoofing patterns are continually changing, and the sophistication of spoofing is increasing.

08 Emergencies now carry higher risk

Even in normal operation, degraded aircraft systems, situational awareness, and higher crew workload creates a stressful and higher-risk operating environment. In the event of an emergency (e.g., engine failure, fire, depressurization), the ability of the crew to safely handle the event is significantly impaired.

Safety Concerns

Aircraft operation and handling



Pilot View southbound on airway UM 688 from RATVO

Aircraft almost enters Iranian airspace without clearance

Dotted area shows area of navigation failures in past 10 days .

Map Date: **28 Sep 2023**

Map © 2023 OPSGROUP Satellite imagery © 2023 Landsat/Copernicus Data © 2023 Google

A depiction of one spoofed aircraft almost entering the Tehran FIR without clearance, close to an active missile base. September 2023.

01 RNP with Contaminated GPS

The risk related to a contaminated GPS Receiver after passing through a spoofing area has not been fully addressed. Even if the GPS receiver seems to have recovered post-spoofing (**appearing normal to the crew**), it may retain contaminated system values. This presents the risk of an issue occurring during an RNP approach, particularly in IMC, and aggravated by the lack of a functioning EGPWS.

02 Go-Arounds from unusual altitudes

Flight crew are typically trained in go-arounds at very low altitude, e.g., at the Missed Approach Point, or during the final landing phase. The rate of false EGPWS alerts is leading to go-arounds at higher altitudes, e.g., 4000 feet, which are not typically trained. **This increases risk of handling errors, level busts, and in the extreme case, potentially loss of control inflight**. This concern is backed up by observations from simulator instructors during GPS Spoofing training.

03 Incorrect runway selection

Several crew reports of **almost landing on the wrong parallel runway** during visual approaches. GPS Spoofing leads to a Map Shift, which subtly leads crew to the wrong runway.

04 Nuisance alerts in critical flight phases

In many reports reviewed by the Workgroup, there have been multiple spoofing-related EICAS warnings in the later stages of approach and landing. **This leads to distraction**, a "heads down" problem-solving period, and uncertainty. Similarly, in many cases EGPWS warnings have continued from cruise altitude to landing, creating disorientation and stress.

05 Heads-down Taxi

At airports in jammed or spoofed areas, warnings may be triggered relating to RWY safety, navigation accuracy etc. This leads to longer periods of "heads-down" taxiing.

06 Weather radar failures

Multiple crew reports of weather radar failure or unusual behavior after spoofing, leading to **inability to detect Cb cells (Thunderstorms)**. Some crews report trying to use lightning flashes to visually observe cells instead. Others report large cells dead ahead not showing.

07 Enroute navigation

The onset of spoofing has led to sudden and unexpected turns off track due to spoofing, leading to lateral deviation from clearance, and loss of ATC separation.

08 Unplanned entry into Danger Areas, Restricted Airspace, and other FIR's

The lack of a clear crew indication of spoofing means that the **aircraft can commence a false turn without crew awareness**. This has led to entry into danger and restricted areas, military airspace, and Standard Instrument Departure (SID) deviations on departure. It has also led to aircraft entering other Flight Information Regions without clearance or authorization, which creates risk of misidentification and in the extreme case, interception or shootdown.

09 Impact on escape routes

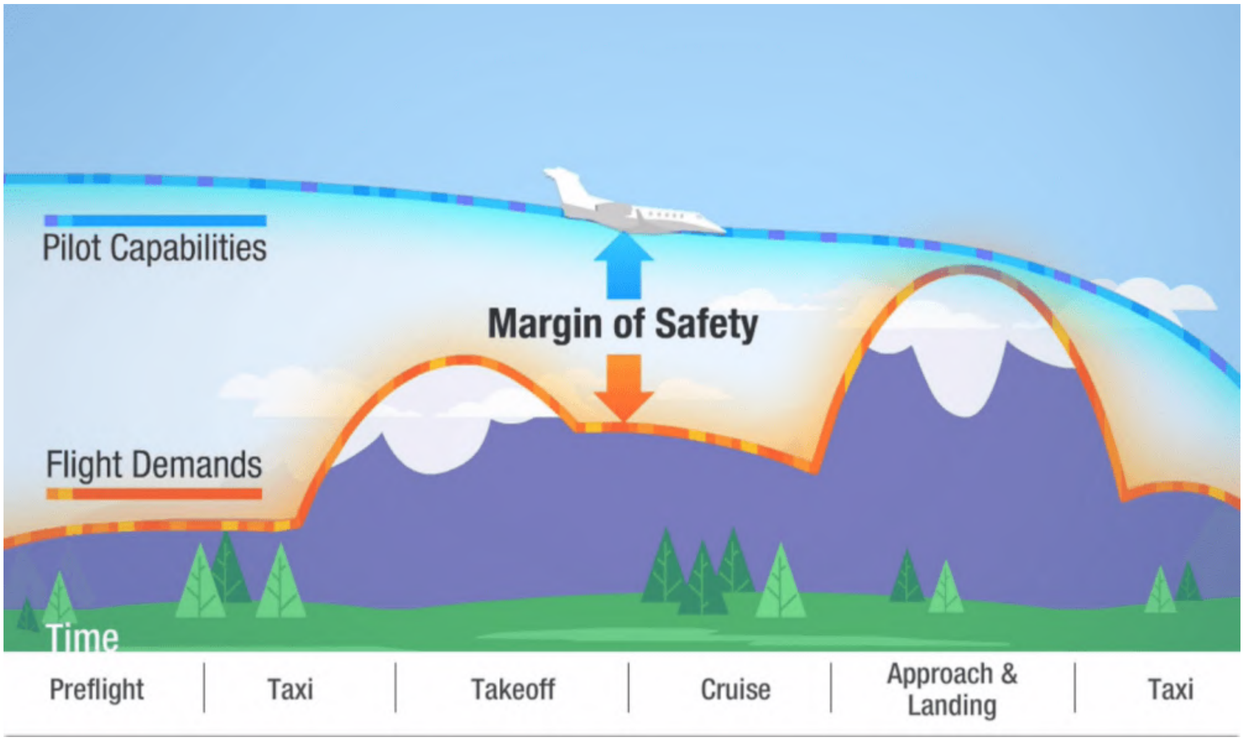
Spoofing renders some RNP approaches from oxygen escape routes unavailable. This cuts down options at challenging airports in high terrain, sometimes leaving an NDB approach as an option.

10 Runway protection systems

Incorrect GPS Location leads to runway overrun system false indications. If not properly identified the system would have called for an unnecessary go around.

11 Complex Go-arounds

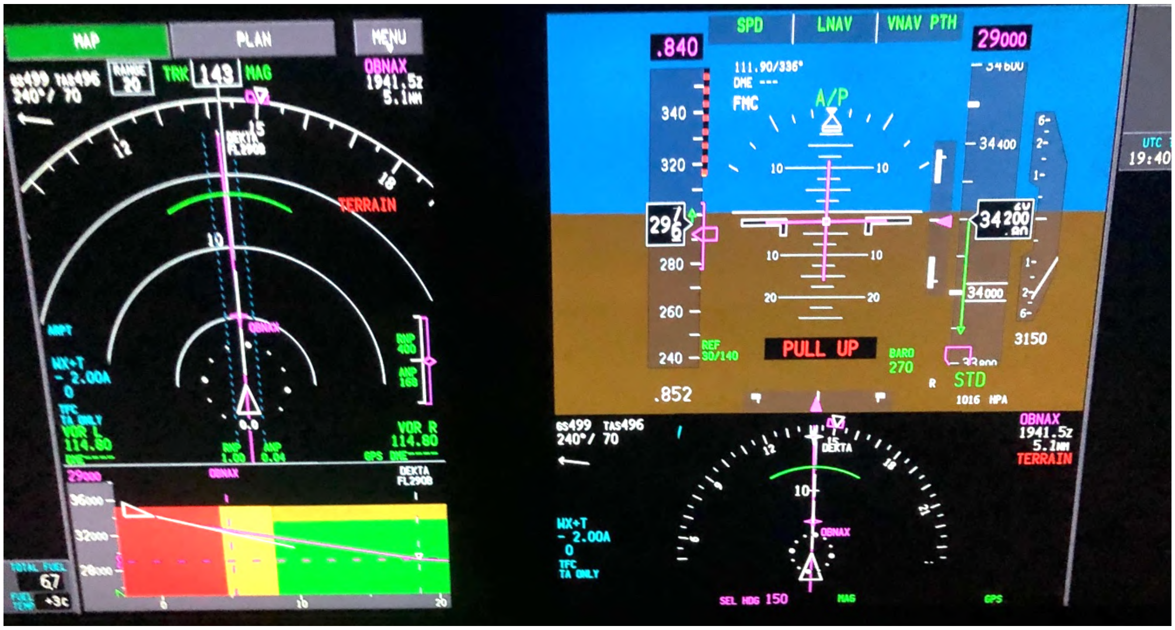
Especially at airport in GPS spoofing areas (e.g., Larnaca, Beirut, Cairo, Tel Aviv), there are a high number of interwoven aircraft systems that can fail, or become unreliable. Many reports from crews detailed **trying to handle multiple failures**, leading to a go-around and in turn further failures. The margin of safety during a complex go-around is at its lowest. If any further non-normal or emergency situation were then encountered (e.g., engine failure), the risk of an accident is greatly increased.



Safety Margins in different phases of flight. Image Source: elearning.flightsafety.com

Safety Concerns

GPWS



The number of false EGPWS alerts has risen dramatically. Depicted above is a typical false EGPWS "PULL UP" alert at high altitude, which is coupled with a loud aural warning that often continues to landing.

01 Many flights operating without EGPWS

GPWS is a critical safety system that over decades has reduced CFIT (Controlled Flight Into Terrain) accidents to very low levels. With every spoofed flight likely to lose the Enhanced, or Look-Ahead functionality of the GPWS system, **the risk of CFIT increases**, especially in light of other system impacts. **Routinely operating without EGPWS, as is now common, is one of the greatest safety concerns**.

02 False GPWS alerts now routine

The high level of EGPWS spurious warnings are now so common that **crews are becoming used to treating warnings with suspicion**, leading to a delayed reaction. This has created a normalization of deviance around GPWS responses.

03 Ignoring genuine GPWS alerts

Genuine GPWS callouts, especially basic-mode GPWS alerts, are at risk of being treated with less gravity.

04 Loss of trust

The previously high level of flight crew trust in GPWS is already eroded. This will continue as more crews are exposed to GPS Spoofing.

05 Inadequate procedures

Procedures for EGPWS responses do not take into account the current issues. OEM guidance is in some cases strict, yet does not account for all cases.

06 Low energy GPWS responses

False EGPWS warnings at cruise altitude, and in other low energy aircraft states, create the risk of an automatic or startle response **potentially leading to aircraft stall**. In some reports, crews report that aircraft speed reduced rapidly into the red. This is exacerbated by strict application of OEM policy for some operators.

07 Cabin Injuries

Unnecessary reaction to false EGPWS alerts in cruise phase of flight, when cabin crew and passengers are not wearing seatbelts, has the potential to lead to cabin injuries.

08 Startle effect and distraction

Unexpected false EGPWS callouts easily create **startle effect**, leading to inappropriate crew reactions. In many cases these alerts continue all the way to landing, with crew unable to silence them, creating a highly distracting environment.

Safety Concerns

Procedures and Training

01 Lack of simulator training

Very few operators have simulator sessions to adequately train for GPS Spoofing. Effects are hard to replicate in the simulator. As such, crews do not have any level of training to "fall back on" for the common effects, e.g., GPWS response handling, go-around at unusual altitudes, decision making, etc.

02 Inadequate briefings

In most cases, there is a **lack of a procedural format for briefings on GPS Spoofing**, including Pre-flight, Takeoff (where on-ground spoofing is expected), Approach, and in-flight before spoofing. Crews are including some discussion of spoofing under "Threat and Error Management", but the lack of clear procedure means critical scenarios may not be discussed. Proper briefings reduce risk of startle effect and poor reactions.

03 Not incorporated into procedures

Currently, the majority of GPS Spoofing guidance is presented to crews via company memos and ad-hoc PDF documents. Often, these are insufficient, incorrect, and sometimes misleading. The **lack of comprehensive guidance built into crew manuals (e.g., FCOM) and the QRH**, create a safety concern.

04 Making up own procedures

Due lack of guidance, **crews are coming up with their own procedures** and potentially aggravating their situation. Similarly, operators have also had to create their own procedures which may not be risk-assessed or fully informed.

Safety Concerns

Human factors and CRM

Safety Concerns

01 Increased Crew Workload

GPS Spoofing events, especially unexpected, plus aircraft system impacts create **rapid increase in crew workload**. This is particularly concerning for single-pilot operations.

02 Normalization of risk

Due to now commonplace encounters of GPS spoofing impacts, there is a gradual, insidious **acceptance of increasingly higher risk** at organizational level. Small changes and new behaviors that were slight deviations from the normal course of events gradually become the norm, providing a basis for accepting additional deviance and, typically, higher risk.

03 Spoofing fatigue

Feedback from crews affected by GPS Spoofing indicates that "Spoofing fatigue" is now common: "We see this all the time now, so we stop reporting, and become used to it". This creates room for complacency and reduced guard against errors.

04 Scan quality reduced

Because of the high number of EICAS warnings related to spoofing, crews have reported missing other important (and valid) warnings. The quality of the scan is reduced.

05 Situational awareness reduced

The impact of GPS Spoofing on primary navigation capability, and uncertainty/doubt as to which information is reliable, and which is not, reduces the overall situational awareness of the crew.

06 Crew disagreement and conflict

Due to lack of clear procedures, and lack of specific spoofing training, crew disagreement over the best course of action can lead to **cockpit conflict**. This can have a major impact on CRM. Some of these disagreements may occur at low altitudes close to ground level.

Safety Concerns

Air Traffic Control

01 Level busts & loss of separation

Especially in spoofing areas, ATC input to the Workgroup presented numerous reports of separation loss, due to false EGPWS alerts leading to uncoordinated climb.

02 Lateral deviation

During spoofing, aircraft are turning unexpectedly without ATC clearance, deviating laterally from the cleared route. This can rapidly lead to a loss of separation. In some FIR's, aircraft are also at risk of quickly **entering danger or military areas** without authorization. At the same time, crew are often unaware of the navigation system error that causes these turns until alerted by ATC.

03 Increase in ATC workload

Especially in spoofing areas, the **increased requirement for radar vectoring** can quickly lead to a higher workload for the sector controller. In one FIR, 382 cases of radar vectoring required due to spoofing were recorded, over a 6-month period. This in turn can create sector overload.

04 Surprise climbs

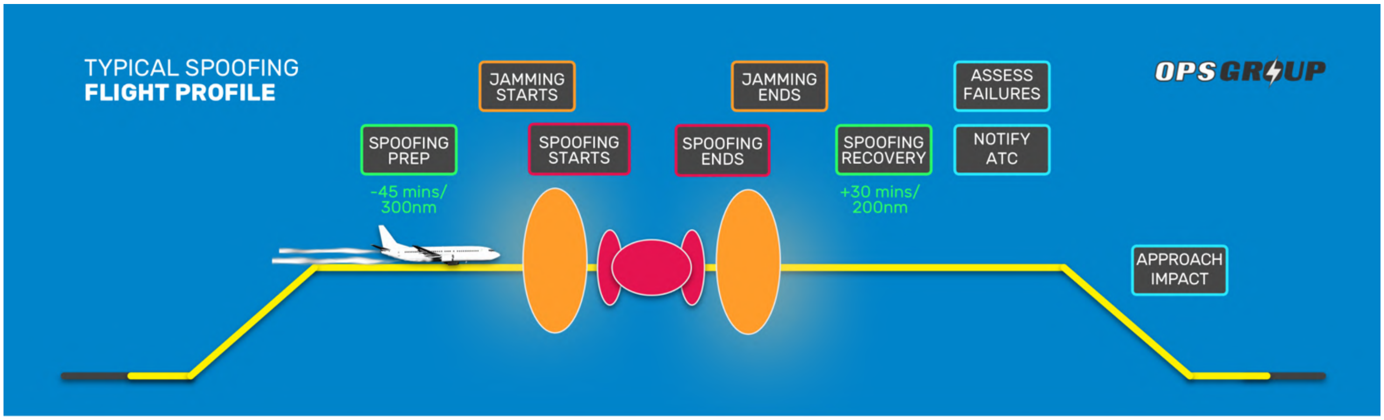
A major concern for ATC in spoofing areas is the issue of unanticipated EGPWS responses, at altitudes and positions not normally seen. This means that especially on approach, **any aircraft could suddenly commence a high-energy climb**. Traffic above is not protected in the same way that it might be when above a missed approach area, for example. Further, in the event of a surprise EGPWS response, TCAS RA inhibition during EGPWS response limits the conflict resolution dialogue between concerned aircraft.

Crew Guidance

If you are operating a flight into a spoofing area **tomorrow**, this guidance will help to mitigate the impact of GPS Spoofing.

This is based on best practices collected from the flight crew participating in the GPS Spoofing Workgroup, as well as OEM and other expert input.

Nothing here is intended to replace or override company procedures, OEM advice, or legal requirements.



Pre Flight

- Refresh systems knowledge
- Crew Briefing: Spoofing plan
- IRS alignment

Pre-Spoofing

- Rebrief plan, signs of jamming/spoofing
- System prep (eg. GPS Off)
- Monitor sensors
- Consider contingencies

Spoofing

- Expect jamming, then spoofing
- May be multiple cycles
- Conventional nav
- Report to ATC

Recovery

- Be certain GPS interference finished
- Re-select GPS sensors
- Assess failed systems and impact

Enroute

- Oceanic: advise ATC early of failures
- CPDLC , ADS-C, Wx Radar, may remain failed
- Review EGPWS actions
- Consider contingencies

Approach

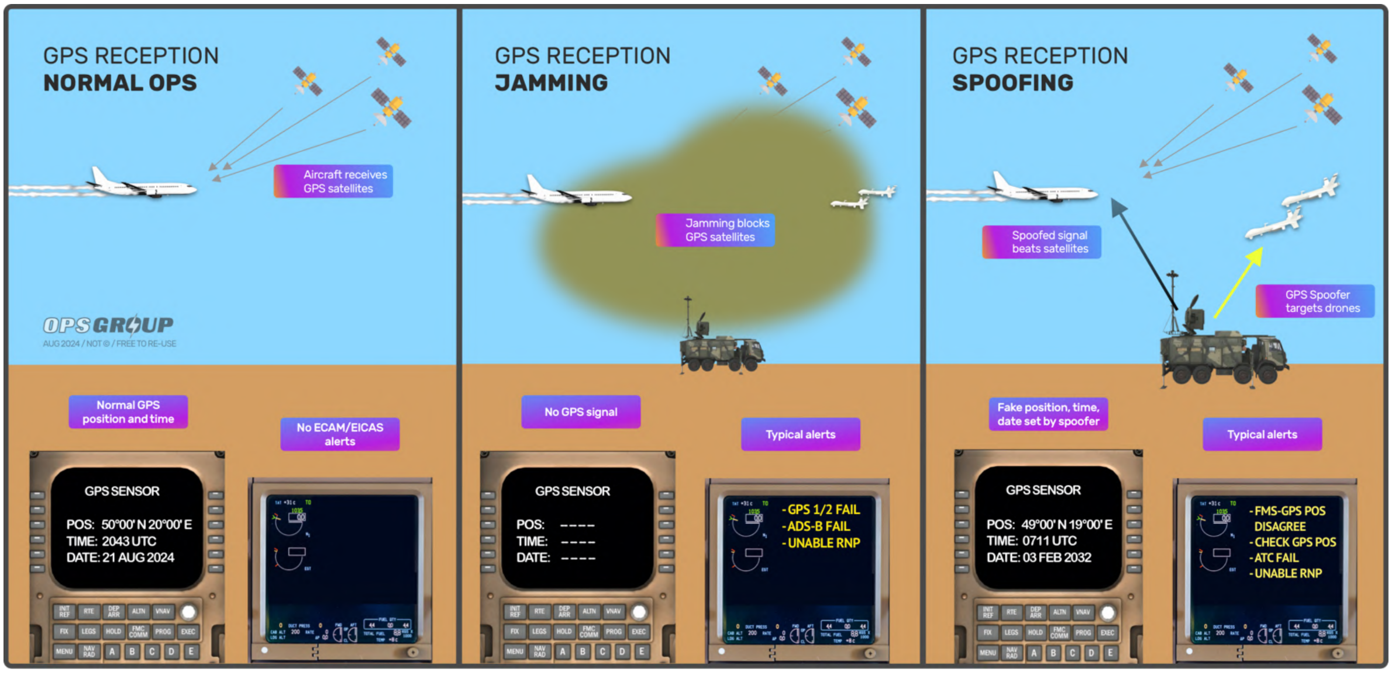
- Anticipate system issues, false EGPWS, EICAS warnings
- Check RNP capability
- Brief spoofing impact on app.

Post Flight

- Report spoofing
- Tech log
- Maint: GPS hard reset may be req'd

GUIDANCE OVERVIEW

REFER TO FULL MITIGATION LIST
GPS SPOOFING WORKGROUP 2024



Pre Flight

Pre-Flight Briefing

For flights into known spoofing areas, include GPS Spoofing as a full briefing item.
Consider:

- Likely entry and exit points of spoofing areas
- Intentions before, during, and after spoofing
- Availability of ground-based Navaids
- Likely system downgrades/losses (e.g., EGPWS, Weather radar, CPDLC, RNP)
- Expected indications of jamming, indications of spoofing
- Contingency planning (e.g., Engine failure, depressurization) in spoofing area
- Impact of spoofing on RNP requirements later in flight

Spoofing Maps

Check online spoofing map for latest locations of active spoofing. Knowing where the spoofing is happening is the best mitigation. (e.g., SkAI Live GPS Spoofing Tracker Map)

GPWS

Specifically review likely EGPWS impact, brief actions for EGPWS alerts in cruise, use of Terrain Override, EGPWS alerts on approach below MSA. Plan action in case of repeated EGPWS alerts on second approach in case of EGPWS response. Review difference between basic GPWS alerts and enhanced/Look-Ahead alerts. Be fully prepared for unusual EGPWS behavior.

IRS

Perform a full IRS Alignment for each flight into known spoofing areas. If departing from an airport within a spoofing area (e.g., LCLK, LLBG, OLBA), perform manual IRS alignment. Caution risk of IRS automatically taking GPS position.

Flight Planning

If practical, file airways associated with ground-based navaids. Review GPS required routes, RNP-1 or -2 airways. Consider alternate routes further from the spoofing area. Review forecasted Cb activity, considering Weather Radar failure is possible. Consider if destination requires RNP approaches.

Contingencies/Emergencies

Consider the impact of spoofing on a diversion while in the spoofing area, or afterwards. Conventional arrival and approach / missed available or daylight VMC from MSA down. Review safe altitudes enroute (MEA/MORA) and at destination/alternate on approach (MSA).

Refresh Technical Understanding

Review difference between GPS Spoofing and GPS Jamming. Know which aircraft systems use GPS (long list!). Loss of ADS-B, SVS, GPWS etc. is not possible to be avoided. Refresh conventional navigation skills, be aware that most enroute airspace isn't actually RNP airspace. Spoofing takes place in areas with low Navaid coverage - may be many hundreds of miles between DMEs and VORs. Understand difference between Conventional/Standalone IRS and Hybrid IRS (B787, G650 etc.).

Synch watches

Synch mechanical watch to known source (e.g., iPhone) at dispatch, in preparation for aircraft clock failure.

NO-TAMS

Don't rely purely on NOTAMs to give comprehensive warnings of spoofing locations.

Crosscheck MEL items

Consider the impact of any MEL (Minimum Equipment List) items. Review impact of unserviceable system items in light of expected GPS Spoofing impacts, especially any inoperative radio navigation items.

Operations at airports WITHIN spoofing areas

- Expect on-ground spoofing, which creates greater risk of system impacts

- **IRS Alignment**: Turn off the GPS receiver via the FMC prior to aligning the IRS, and carry out a manual alignment. Be vigilant for automatic capturing of the spoofed GPS position during alignment.

- Do not plan GPS/RNP approaches, SIDs, STARs, into/out of known spoofing areas

Pre-Spoofing

Prepare for spoofing

Commence preparation and system setup well prior to first expected spoofing location. **Spoofing area ETA -45 minutes, or 300 nm is suggested**.

- Consider declining direct routings to remain on airway, especially if airway is based on Navaids.

- Evaluate emergency descent and diversion options with regard to spoofing impact on systems

Re-Brief plan

A quick re-brief of actions when spoofing is encountered. Intentions, and expected systems loss, e.g., ADS-B, CPDLC. Re-brief EGPWS actions in event of alert in cruise.

Monitor

Monitor EPU (Estimated Position Uncertainty) and ANP (Actual Navigation Performance) values. Open Sensor/Pos Ref page for GPS status. Anticipate jamming to commence before spoofing: the typical spoofing encounter now commences with a period of GPS jamming, which makes the GPS receiver more vulnerable to spoofing. Monitor aircraft clock for jumps or changes.

Increase vigilance

- Keep an eye on all aircraft systems for unusual behavior.

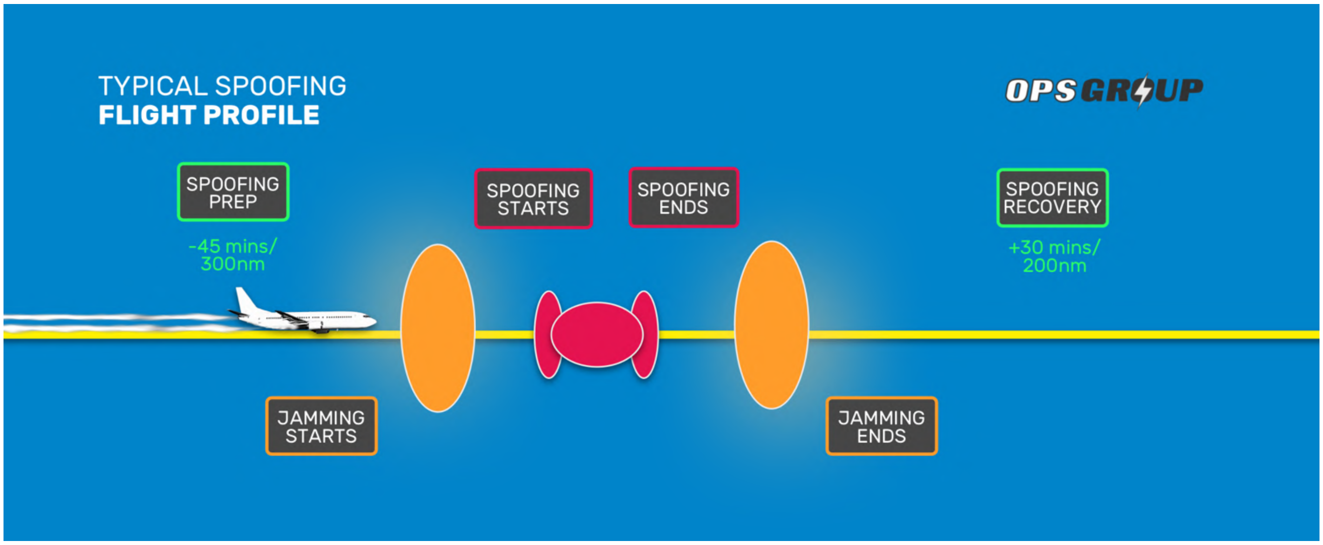
- Monitor aircraft position and navigation system status using all available means, including use of a handheld GPS e.g., Bad Elf, Garmin, iPad/iPhone, EFB. Keep the antenna of the external GPS system in sight of satellites but as shielded from the horizon as possible, using glareshield or aircraft frame. Any disagreement between aircraft GPS and external GPS will suggest spoofing.

- Use an alerting App such as APG's NaviGuard. Regularly cross-check aircraft system indications to standalone systems (e.g., Watch, VOR/DME position, EFB/External GPS) to detect spoofing early.
- Listen out for ATC or other aircraft reports of spoofing
- Be ready to apply systems setup as soon as typical initial warnings occur, in case of surprise/early spoofing encounter.
- Have Nav Log (OFP/CFP) tracks, times, distances ready to assist with manual/DR navigation.
- Keep an eye on GPS date (in sensors page). A date change is a strong indicator of likely problems recovering the GPS receiver post-spoofing.

Set up aircraft systems

- Always follow OEM and Operator Procedure as primary spoofing setup guidance.
- **De-select GPS input to FMS**. Note that this will only prevent the FMS position from including spoofed GPS values, but will not protect other systems e.g., EGPWS, Weather Radar.
- **Deselect "IRS HYBRID" mode** if applicable.
- **Set the aircraft clock to "Internal" (INT)** / manual, if possible, to protect CPDLC and other datalink functions.
- If procedure approved - **Inhibit EGPWS Look Ahead mode** to prevent false alerts at cruise altitude.
- Stow **Head Up Display** and do not use.

Within Spoofing Area



Typical indications of Jamming

It is common for jamming to precede spoofing. Jamming will result in the loss of GPS Signal only. The time from jamming to spoofing varies.

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

Typical indications of Spoofing

Unlike jamming, a GPS signal is present, but it has fake information. False GPS position, time, and date information will be processed by the GPS receiver as being valid. As soon as this is fed to other systems, failure messages will begin.

- **Rapid EPU or ANP increase**
- **GPS position** and IRS or FMS position disagree caution message
- **Aircraft Clock time changes**, or difference between Capt/FO clocks
- **Transponder failure**: EICAS/ECAM "ATC FAIL"
- **Autopilot turns aircraft unexpectedly**
- **ADS-B Failure/Warning**
- **Synthetic Vision** reverting to blue over brown
- **Loss of enhanced display**, such as display of terrain on PDI
- **Wind indication** on ND is illogical or has a major shift - erratic groundspeed
- **GPS position symbol** on ND drifts away from the FMS and the IRS symbols
- **Datalink** (CPDLC, ADS-C) failure warning
- **GPS information on sensor page** shows unusual values: altitude, etc.
- **Handheld GPS** (e.g., Garmin, iPad) **disagrees** with aircraft GPS position
- **EGPWS** audible warning ('Pull Up")
- **GPS 1 and 2 dramatically different** i.e., more than 100 meters, which may also give an ECAM/EICAS GPS miscompare warning.
- **Spoofing Alerting app** e.g., Naviguard gives alert
- **ACARS message** from ground/ops advises of spoofing (based on aircraft downlink message with unusual values).

Actions following confirmation of active spoofing

- **Aviate, navigate, communicate** – back to basics.
- Note the time on personal watch, record on log.
- Check system settings are correct for spoofing protection. Also applies to unexpected "surprise spoofing".
- **Check GPS input de-selected**
- **Check IRS Hybrid mode de-selected**
- **Heading mode**: Consider selecting heading mode to keep the aircraft on track during troubleshooting
- Confirm Nav Source in FMS: DME/DME, IRS, etc.
- **Report to ATC**. Advise ATC of spoofing encounter ASAP. Include position so that other crew on frequency are aware.
- **Request ATC vectors** or confirmation of correct position and track if required.

- If company procedures allow, **inhibit EGPWS at cruise altitude** (TERR OVRD). This avoids false "PULL UP" etc. warnings triggered by spoofed altitude data.
- Use **Conventional Navigation**
- Check Aircraft Clock Time and compare to current time.
- Check **GPS Date** on sensors page. A change of date, especially forward in time, is likely to create greater GPS receiver problems after spoofing.
- **FMS Auto-tune** may not function correctly (uses GPS to check Navaid position).
- **Set reminders** based on waypoint or coordinates (not time) to reverse all system settings changed for spoofing.

Recovery

Most spoofing encounters can be fully recovered from in flight. However, an increasing number of aircraft are left with severe impacts to navigation, communications, and safety systems (e.g., EGPWS) that are not recoverable before reaching destination.

Before beginning recovery, be certain that spoofing has finished. Double check known spoofing location map, and be alert to the possibility that another round of spoofing may occur. Allow a time period of normal GPS readings, e.g., 10 minutes.

Indications that spoofing is complete

The following items may be helpful to identify the end of GPS Spoofing:

On Sensors/Pos Ref page, GPS shows:

- Correct UTC time and date, **and**
- GS (Ground Speed) consistent with TAS, ND, **and**
- Consistent position and altitude

Actions after exiting spoofing area

- **Re-select GPS** sensor input to FMS
- **Assess** all systems for failures, especially Weather Radar, CPDLC/Datalink,
- If required, and if procedure exists/allows, carry out **in-flight reset of MMR/GPS Receiver**
- If required, and if procedure exists/allows, carry out **in-flight reset of GPWS computer**

ATC

- Advise ATC of any relevant systems remaining failed, e.g., Nav, CPDLC, ADS-C and impact on navigation (e.g., Unable RNP)

- Disregard any CPDLC mandate for domestic FIR's – airspace entry will not be denied.

- **If planning an oceanic crossing** with degraded RNP or Comms systems, advise the first oceanic ACC well before Oceanic Entry. For example, Shanwick requests a freetext remark in the RCL message at OEP -90, "RMK/RNP 10 ONLY DUE GPS INTERFERENCE / NO CPDLC"

- **For the NAT HLA**, note that RNP4 is required for PBCS tracks, as well as CPDLC and ADS-C for the RCP/RSP requirement. Elsewhere in the HLA, RNP 10 is the minimum, but RNP4 is often used for tactical separation outside the NAT PBCS Tracks. If you are RNP10 only, **expect lower crossing altitudes and reroutes**.

- Request to follow STARs (/SIDs) based on conventional navaids.

- Avoid/decline RNP approaches.

Destination/Alternate Approach considerations

- **Even if the GPS receiver appears normal** after spoofing, there is a risk of later failure or incorrect behavior. This is because the spoofing may have contaminated the receiver settings. In most cases, only a hard reset will guarantee receiver integrity.

- **Avoid RNP approaches** unless there is certainty that all systems are operating normally. Check missed approach for any RNP/RNAV requirement.

- **Advise ATC** of your earlier GPS interference, e.g., "Due to earlier GPS interference, unable xxx approach, request xxx approach". This will also give ATC a heads-up to monitor your tracking more closely.

- **Brief intentions re. GPWS responses.** Expect false EGPWS alerts, but re-brief to be clear on difference between GPWS basic mode alerts (Radio Altimeter based) and EGPWS alerts (GPS altitude based). Ensure all basic GPWS mode alerts are followed without delay, as these are not affected by spoofing. Brief intentions for different alert types.

- **Brief possible ECAM/EICAS alerts** on descent and approach, especially ones that may occur on final approach but can be disregarded, e.g., RNP related warnings.

- **Check alternate** non-GPS approach availability.

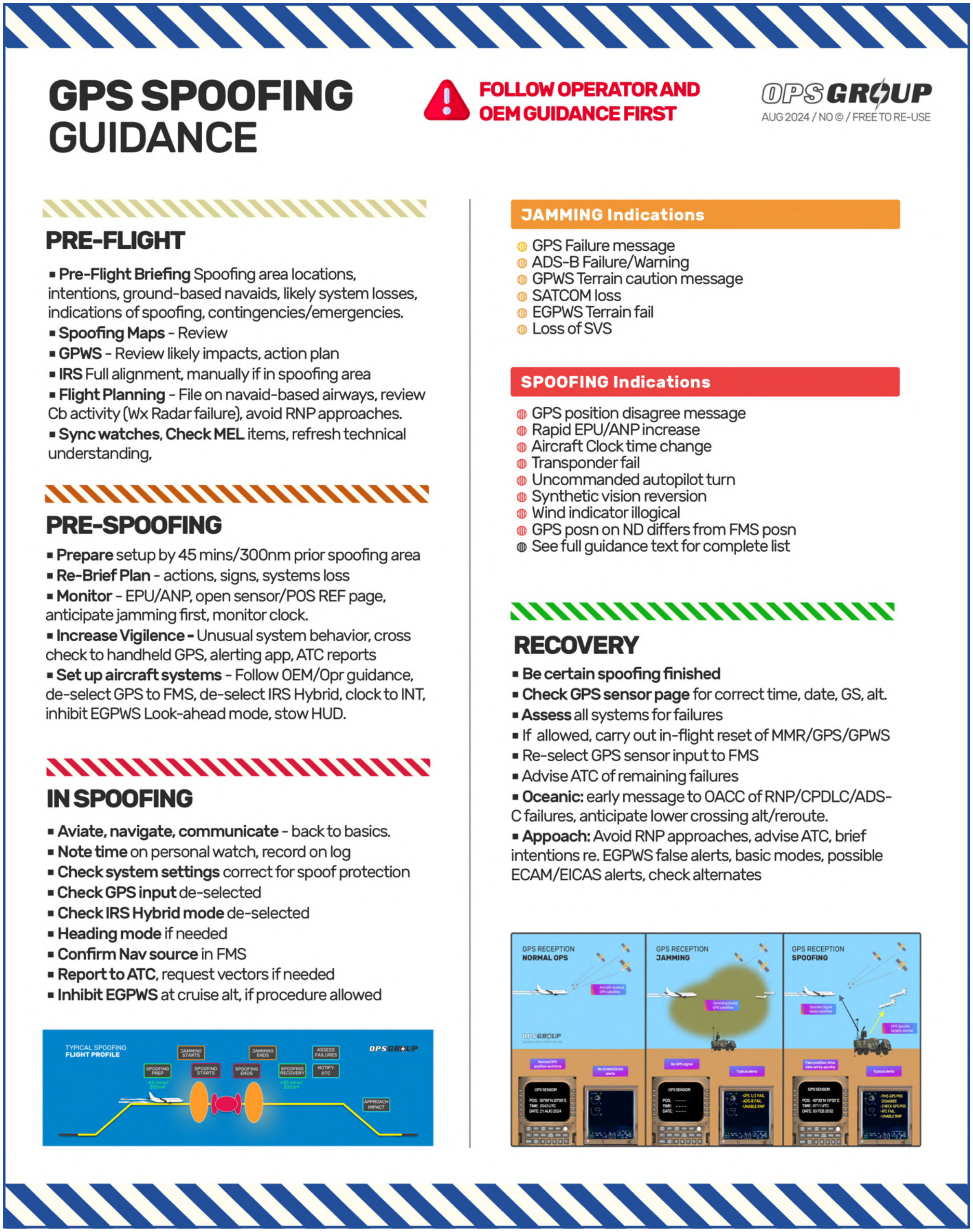
Post Flight

- **File an Air Safety Report** for tracking of the GPS Spoofing problem.

- **Tech Log:** Note any GPS Spoofing in the aircraft tech log each flight, to ensure a hard reset of the GPS / MMR is carried out

- For any unusual system impacts, send data to avionics manufacturers e.g., Honeywell, Collins.

A full-page version of this **one-page guidance summary** is available in the Appendix.



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

Solutions

One thing is clear: **there are no easy overall solutions**.

While mitigations can provide some temporary relief from the spoofing issue, longer term solutions to solving the problem are critical.

Consideration must also be given to the potential for a deepening of the GPS vulnerability problem. In mid-2024, we are already seeing a major increase in spoofing and follow-on impacts.

Locations of interference could widen, and impacts could worsen.

What needs to be fixed?

Before presenting potential solutions to GPS Spoofing, the first question must be: **What is the problem?**

In the "Impacts" section above, there are two distinct areas:

13. **GPS Unavailability** due to spoofing and/or jamming, leading to loss of GPS-based navigation capability, and some system losses.

14. **GPS Contamination** due to spoofing, leading to downline systems failures including FMS, EGPWS, Datalink, RNP, and creating unsafe aircraft states and situations.

Solving the contamination issue is more pressing than the unavailability issue, due to the raft of safety concerns surrounding the former.

GPS Contamination problems

1. There is no specific flight-deck system **indication** to crew that they are being spoofed, and limited options for crew awareness from other sources.

2. There is no ability to **isolate** the GPS Receiver from other aircraft systems, other than the FMS. As such, there is no protection that can be applied to critical systems, e.g., EGPWS

3. There is no ability to **reset** contaminated safety systems, e.g., EGPWS

4. There is limited ability to **reset** the GPS Receiver in flight, and it may not clear the issue.

5. A contaminated GPS receiver may appear to recover, but still fail later in flight.

6. There is currently very little ability to determine **where** spoofing is happening, especially while in flight.

GPS Availability problems

1. GPS as used by civil aviation is highly vulnerable to interference.

2. Availability of ground-based Navaids is slowly reducing.

Potential Solutions

1. Awareness maps
2. On-board detection and alerting
3. In-flight resets
4. Avionics improvements
5. Design changes

1. Awareness maps

The greatest *tactical* protection against spoofing is a clear indication of where to expect it, allowing crew to set up aircraft systems in time to protect some systems from spoofing (e.g., FMS, IRS, Datalink)

15. A live GPS spoofing and jamming map that displays affected areas, the number of affected aircraft, and related statistics is provided by SkAI Data Services in conjunction with the University of Zurich, and Spirent Communications. Both providers offer maps in addition to detection and alerting services that can be integrated into EFBs and other software.

16. GPSJAM.org shows regions of jamming, using indications of degraded ADS-B data. This often means jamming, but could be spoofing, or other reasons. However, at the time of this report, there was no specific depiction of spoofing areas.

17. EASA has an in-house developed spoofing map.

18. A map of spoofing locations integrated into commercial flight planning systems (e.g., Lido, Jeppesen, etc.) would be of great value.

2. On-board detection and alerting

A warning to crew that spoofing has been detected on their aircraft assists in awareness.

- A crew-directed "**Spoofing Alert**" can be sent via ACARS or to an EFB from a variety of suppliers including Spirent, Leidos and SkAI Data Services.

- **ACARS Spoofing Detection**. Several airlines in the Workgroup shared their process for detecting spoofing based on ACARS messages received from the aircraft. They use an algorithm based on the downlinked aircraft clock times. In turn, they can then advise the aircraft via ACARS, that spoofing has been detected.

- APG software has an **alerting app** for personal devices called "Naviguard". Crew report this works well.

- A **handheld GPS receiver** (or tablet/device with GPS) can provide indication of spoofing in progress. If the receiver is intentionally positioned low down in the cockpit such that it only has a direct line of sight to the highest elevation satellites and has no view of the horizon at all, then it is possible that it may not get jammed and spoofed as easily as the externally mounted antennas. Examples mentioned by crew include Bad Elf, Garmin devices, iPhone, EFB map.

- **Geofenced alerts**, e.g., an ACARS "You are entering a spoofing area", could be useful if based on current information.

3. In-flight resets

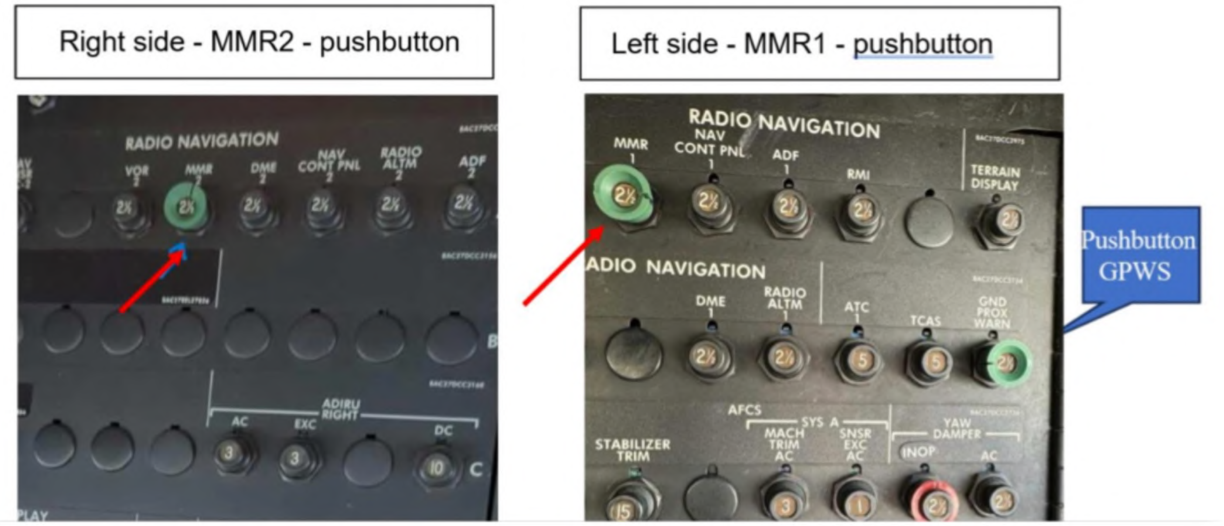
The Workgroup heard both arguments for and against increasing the ability of crew to reset critical systems in flight, through a **circuit-breaker (CB) reset**. Historically, OEM's and authorities prefer to have "crew in seats", and not "away from station", and are concerned about the potential for incorrect CB selection, as well as damage to sensitive CB panels. Further, some aircraft (e.g., A330) have the CB panel outside the cockpit, in the avionics bay, and is thus not accessible in flight.

However, the impacts of a failed GPS receiver and EGPWS system due to spoofing, create the need for a **reassessment of risks vs. benefits**. Additionally, a sizeable number of operators and crews are already carrying out this practice, even in the absence of official approval. A more streamlined, approved procedure would be safer.

- **EGPWS reset via CB**. Even if the GPS Receiver comes back online, the EGPWS still stores incorrect position/altitude information, which is why surprise false alerts come at destination. Terrain Override, or removing the Look Ahead function, reduces the GPWS to Rad Alt based basic modes only. A **crew reset of the EGPWS CB** may be a solution, aircraft type dependent. Anecdotally, operators employing this reset have seen no further false EGPWS warnings later in flight.

- **GPS Receiver (/MMR) reset via CB**. A reset of the receiver in flight typically restores full functionality, and hence RNP and Nav capability, as well as datalink, etc.

- Colored collars can be added to the Circuit Breaker to ease identification, as shown in the image below.



Right side - MMR2 - pushbutton

Left side - MMR1 - pushbutton

Pushbutton GPWS

4. Avionics improvements

This area of potential solutions is already well in progress by some OEM's and Avionics Providers, but with varying timelines. An overview is provided for reference.

- **EGPWS Computer logic**. An update to the EGPWS software could provide better handling of GPS spoofing hangovers. Typically, even if the GPS receiver recovers fully, the EGPWS still keeps some of the spoofed information.
- **GPS Receiver logic - "Big Jump" Gross Error Check**. Typically in spoofing encounters, the GPS position will appear to jump by 60 nm to 200+ nm, in a short space of time. A Kalman Filter style error check should preclude this from being accepted by the receiver. However, because a period of jamming (often) precedes the actual spoofing, the receiver is in a new search mode to find satellites. It hence has no previous reference to see the jump. A software change in the receiver, with an improved algorithm to provide a **tighter restriction** on how much it can trust new GPS signals after a period of unavailability may solve this problem. The same applies to big jumps in **time**. A recommendation would be to enforce receivers to use "warm acquisitions", such that if a receiver loses lock on satellites and tries to reacquire them it verifies that the time stamps and orbital information are very close to those already in memory, else a spoofer warning is raised and the system rejects the new data.

- **Flight Management Computer**. Updated software may assist detection of major jumps in sensor values, before being fed into the FMS position computation.

5. Aircraft systems design changes

Longer term solution:

- Re-design system architecture to **enable isolation** of the GPS receiver from all other aircraft systems. If the GPS receiver can be isolated, then other aircraft systems have protection from false information.

Potential Solutions

The primary concern around GPS availability is the **vulnerability of current civil aviation GPS** Receivers to interference, such as spoofing and jamming. The Workgroup considered various potential solutions. GPS and technical experts offered their opinions, but noted that this is a longer-term set of solutions, many of which need to be assessed further. A summary of areas considered is below:

1. CRPA Antennas
2. Encryption and authentication
3. Strengthening Ground-based Navaid network
4. GPS interference detection products from other industries
5. Military GPS versions
6. Other solutions

1. CRPA (Controlled Reception Pattern Antenna)

Of all potential hardware solutions, the CRPA was heavily favored by the Workgroup as offering the greatest benefit to avoid spoofing.

- The current standard GPS antenna is omnidirectional. A CRPA offers **more specific directional capability**, resulting in the ability to filter out spoofing signals.
- **Military aircraft** are able to avoid GPS Spoofing for two main reasons: they use CRPAs, and encrypted GPS. Encrypted GPS is not currently available for civilian use, but CRPAs could be installed on civilian aircraft.
- **Some airlines have reported already beginning** to investigate the process of installing CRPAs.
- Two challenges to immediate use of CRPA include: ITAR (International Traffic in Arms Regulations) restrictions on US-related products, and potential airworthiness certification requirements.
- The cost of a CRPA antenna is estimated to be in the range of $10,000 - $100,000 USD, but could be less if a group of airlines or operators cooperated to approach a supplier.
- Non-US Manufacturers of CRPAs include Raytheon (UK), and TUALCOM (Turkey).

2. Encryption and authentication

There are currently no encrypted signals available to the civilian sector. Galileo intends to commercialize its encrypted Public Regulated Service (PRS) for specific use cases within the EU member states in the near future.

3. Strengthening Ground-based Navaid network

The industry trend has been to move away from Ground-Based Navaids as much as possible.

However, in light of the exposure of GPS vulnerability, a reverse in this approach is needed. At minimum, the Workgroup considered that a halt to any removal of enroute navaids (VOR, DME) would be sensible.

The negative impact on future plans for RNP-only airports or airspace is already clear.

4. GPS interference detection products from other industries

Other industries suffer from GPS/GNSS jamming and spoofing too, and a list of products used is below. Many of these systems are designed to protect critical infrastructure, in many cases communication networks that use GNSS for synchronization. They detect jamming and spoofing by detecting changes in the GPS/GNSS clock using expensive clocks/oscillators and the fact that these systems are in a fixed position. Not all may not be applicable for aircraft or aviation.

Some of the products listed below are software enhancements to a GNSS receiver system. They would need to be adapted for use in certified avionics, but these solutions and techniques being developed by traditional aviation suppliers can be used to provide more resilience to jamming and spoofing.

- BroadShield (Safran Federal Systems) - set of algorithms for jamming & spoofing detection
- BroadSense (Safran Federal Systems) - jamming & spoofing detection sensor
- BlueSky GNSS Firewall (Microsemi) - software for detection and protection of GNSS RFI, intended to be installed between the existing GNSS antenna and GNSS receiver system
- DRACONAV (by FDC) - GNSS module for safe PNT determination with resilience against GNSS jamming & spoofing, combination of hardware and software, able to detect and consequently exclude the compromised signal from further processing
- AIM+ (Advanced Interference Mitigation and Monitoring) technology in GNSS receivers by Septentrio - ensures resilience against jamming and spoofing
- Supercorrelation (Focal Point Positioning) - a software upgrade for GNSS receivers that allows them to determine signal arrival angle without the need for a CRPA or any antenna changes, and provides anti spoofing and spoofer localization capabilities

- SecureTrack (By Nexteon/SeRo Systems) for jamming and spoofing detection; jammer location; combination of hardware and software; passive detection.

5. Military GPS versions

An obvious question is, if the military are impervious to GPS Spoofing, can we copy some or all of what they do?

Military use encrypted signals, such as P(Y) and M code. Because these are encrypted, they can't be spoofed in the same way as the open civilian signals. Aircraft equipped only with military GPS store crypto keys, and they only receive GPS from the source that has the key. The keys expire in the same way as the FMS nav database, and without the crypto, it cannot be used.

They also use receivers that are better designed to recognize and reject spoof signals.

Military aircraft also use a special type of CRPA antenna that removes spoofing. Only a few CRPAs are capable of doing this. CRPA can detecting interfering signals on GPS frequencies and blank out the reception from that direction.

There are also military platforms with no access to the encrypted signal, which instead use a CRPA to provide their protection while using the public GNSS signals.

6. Other solutions

Better GNSS Receiver signal processing

- Spoofer mitigation using enhanced GNSS receiver signal processing (e.g., Synthetic Aperture Processing)

Multi-Frequency Multi-Constellation (MCMF) GNSS Receivers

Most avionics today are still using just the L1 GPS band. Adding other constellations and frequencies adds accuracy and integrity under normal operation, but **they add no realistic protection against jamming and spoofing** in the medium and long term, unless specific spoofing algorithms are added to their design.

The vulnerability of GNSS to jamming and spoofing is caused by the very low power transmission (50W) of the distant sources (20,000km) and the open-source nature of the signal content. Adding more weak open-source signals from space does not protect against nearby high-powered jamming and spoofing sources, even if today it is the case that one of the frequencies or constellations are not being jammed or spoofed.

It is not technically challenging to jam another GNSS frequency or spoof another open GNSS signal structure. If a simple omnidirectional antenna is used by the receiver, then the bad actor will always succeed in jamming when they just need to overpower a 50W transmission from 20,000km away. Protection from jamming is best provided by either disabling the source of the jamming signal, or actively nulling it out using a CRPA or similar "smart antenna". The use of signal authentication allows spoofing to be detected and the use of signal encryption prevents spoofing from occurring.

Use of other GNSS frequency bands (e.g. L5) and other GNSS constellations

Typically, GNSS satellites operate in three Radio Frequency bands: L1, L2, and L5. While most existing GNSS satellites operate in the L1 or L2 bands, newer satellites are being developed that operate in the L5 band. Use of the L5 band has been suggested in some places as a potential solution, and that the L5 band might be "immune" to spoofing.

However, while it may be true today that some GNSS frequencies are not currently being targeted for jamming and that some GNSS constellation signal broadcasts are not being spoofed, using any of these publicly-accessible GNSS signals and frequencies is not a viable long term method of protection.

It is equally easy to jam any GNSS frequency and to spoof any unauthenticated and unencrypted GNSS signal. L5 is definitely not immune to spoofing. There is no inherent authentication or encryption. Also, none of the GPS L5 signals are yet certified as safe to use and will not be until the very late OCX ground segment upgrade is completed.

The most likely reason for very little L5 jamming and spoofing happening at the moment will be partially due to energy budget and partially due to legacy hardware. The spoofing transmitters have a finite max power that determines their range. If you have to jam L1 and L5 simultaneously then you divide that max power among a wider set of frequencies and reduce your maximum range of effectiveness. So until the spoofers feel a need to broadcast on L5 they won't waste the range that they have right now. When they do have a requirement to jam and/or spoof L5 they will not have any significant technical barrier preventing them from doing so.

Similarly, it may be the case today that a subset of the GNSS constellation signal types is being spoofed and some are not, but relying on those currently not being spoofed is not a viable long term solution. All of the publicly-available, unauthenticated and unencrypted GNSS signals can be spoofed using similar hardware and software to those being used today to spoof GPS L1 signals.

Alternative sources of GPS-quality PNT

In the much longer term, alternatives to GPS-quality sources of Position, Navigation, and Timing (PNT) could be adopted by aviation.

Recommendations

The WorkGroup has issued the following recommendations regarding GPS Spoofing.

These are not directed at any one authority or organization, but highlight the major issues that need attention.

01 Safety

Recommendation: High priority should be given to **solving the impact on EGPWS** system architecture, through:

a. A fix for the impact on the EGPWS system from spoofing, and/or
b. Ability to reset the EGPWS system in flight and restore functionality

02 Safety

Recommendation: An **avoidance of GPS-required approaches** after a spoofing encounter, even with an apparently restored GPS receiver, **until there is certainty** that there is no residual risk of a contaminated GPS Receiver. This includes all RNP approaches, and any approached involving Synthetic Vision or HUD's. The concern is that even if the GPS Receiver appears to be back online, and showing apparently normal readings, the Ephemeris data is possibly still corrupted through spoofing. In turn, there is a significant risk that satellite readings further downroute will be incorrect.

03 Safety

Recommendation: A review of the ability to fly RNP -4 (Oceanic), or RNP -1, -2 (Enroute), with a possibly contaminated GPS Receiver after a spoofing encounter. Same reasoning as Recommendation #2.

04 Training

Recommendation: Urgently add **simulator handling training** for EGPWS responses, including:

a. **Go-arounds** at unusual altitudes/positions (e.g. 4000 feet)

b. EGPWS response in **low energy states**

05 Training

Recommendation: Airlines and Operators should urgently add an **e-learning module** for Flight Crew on GPS Spoofing, to ensure all flight crew are fully aware of the impact, mitigations, safety risks, and best practices.

06 Training

Recommendation: Improve Technical information available to flight crew on GPS-related aircraft systems. Current aircraft manuals and crew training lacks detail, which leads to incorrect assumptions on impact by the flight crew.

07 Training

Recommendation: Improve general Pilot awareness of the topic of GPS Spoofing in general, including mitigations, risk factors, safety concerns and technical understanding.

08 ATC

Recommendation: Urgently circulate awareness to Air Traffic Controllers, especially Approach controllers, to anticipate GPWS responses in/at previously uncommon locations and altitudes, due to false alerts.

09 ATC

Recommendation: Urgently introduce specific phraseology for GPWS response maneuvers, similar to existing phraseology for TCAS responses. This is recommended in order to direct immediate ATC attention to surprise GPWS responses, and better protect conflicting traffic.

10 ATC

Recommendation: Clarify the altitude to climb to after a GPWS response. Currently there is no standard procedure. Pilots may choose MSA, or some other altitude or level.

11 ATC

Recommendation: (Airspace design) Re-assess the phasing out of Ground-based Navaids, and a review of long term impact of GPS vulnerability on airspace design and approach procedures.

12 ATC

Recommendation: That the content of **NOTAMs** warning of GNSS interference be improved so as to be operationally useful to flight crew, instead of blanket FIR "Expect Spoofing/Jamming" NOTAMs.

13 Procedures

Recommendation: Revise standard pilot GPWS response procedure as follows:

a. Instead of the immediate reflexive response as currently trained, allow for a short period of evaluation (even 5 seconds) to determine correct response (VMC/IMC, Alert at cruise altitude, etc.). This avoids the risk of GPWS response in a low-energy state, or other avoidable responses. A memory item is suggested.

b. Create a clear procedure for repeated false EGPWS warnings on approach, to avoid crew getting stuck in a repeating loop where the same approach flown again, will likely lead to the same false EGPWS warning.

14 Procedures

Recommendation: Shift the focus of GPS Spoofing procedures from company memos, bulletins, PDF's, etc., to full incorporation into published manuals (FCOM, QRH).

15 Mitigation

Recommendation: Provide cockpit crew a means of in-flight warning of active GPS Spoofing (and Jamming). This would ideally be integrated into aircraft system architecture in some way: EFB, FMS software change. Alternatively, an automated ACARS message sent when spoofing is detected (e.g., Clock shift), or via an App.

16 Mitigation

Recommendation: Develop an easily accessible Pre-Briefing GPS Spoofing Location Map that can show the dispatcher, and flight crew, where spoofing has been happening in the days/weeks prior to flight. Knowledge of where spoofing is likely to occur is the best tool to allow for mitigations to work effectively.

17 Mitigation

Recommendation: Add a spoofing map layer to the presented flight plan route in Flight Planning Systems (e.g., LIDO, Flightkeys, Navblue), in the same way as showing turbulence, icing, etc. This would provide excellent additional awareness for flight crew.

18 Mitigation

Recommendation: Develop a trend-analysis tool to highlight changes in GPS Spoofing locations, patterns, frequency and intensity.

19 Mitigation

Recommendation: Provide crew with the option of a handheld GPS receiver product (standalone, in EFB, or iPad, etc.) on the flight deck, to improve detection capability and situational awareness. Several low-cost products exist, and in combination with a shielded antenna location, these can provide both an un-spoofed GPS position and awareness of when spoofing is occurring.

20 Mitigation

Recommendation: Increase industry co-operation and information sharing, with regard to spoofing reports, lessons learned, mitigations, and potential solutions. Further, that the industry work together to create a spoofing-detection algorithm via ACARS.

21 Mitigation

Recommendation: Remove the Controlled Pattern Radiation Antenna (CRPA) from ITAR export restrictions, even if only for use with specific certified avionics, or limited to a reasonable number of elements. The Workgroup identified the CRPA as the most likely hardware solution to solve the GPS Spoofing impact on GPS Receivers

22 Considerations

Recommendation: That major consideration be given by the industry to the similar insecurities and vulnerabilities in aircraft communications and surveillance systems. In particular, the unencrypted access to ACARS, and the public availability of aircraft position information via ADS-B, should be replaced with secure systems. This is not without significant investment in infrastructure, but the industry should take all possible steps to rapidly move to a more secure operating environment.

22 Considerations

Recommendation: Establish the requirement that all future GNSS receivers for aviation must be capable of using signal authentication schemes as and when they become available (e.g. Galileo OSNMA). Further, establish the requirement that all future GNSS receivers for aviation must be capable of rejecting signals that are being received from the wrong azimuth and elevation, with via software or hardware (e.g. CRPA)

24 Considerations

Recommendation: Deployment of new space based GNSS solutions that are more resilient to attack. This could be augmentation of the existing MEO satellites with LEO or public/private partnerships to use existing space based signals for PNT.

25 Considerations

Recommendation: That aircraft operators work together, rather than individually, to approach equipment manufacturers for solutions (e.g. for a CRPA). This would reduce overall cost, and provide the manufacturer with greater imperative and interest to work on bespoke solutions for the aircraft industry.

Appendix

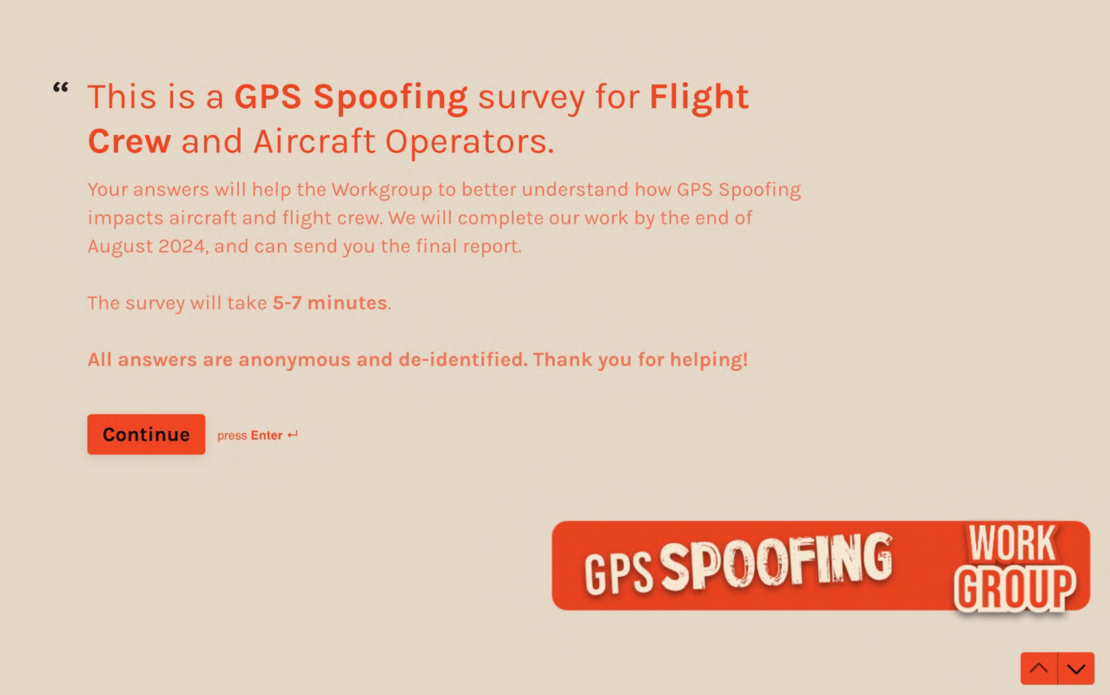
A. Flight Crew Survey Results

This section contains a full review of the Flight Crew Survey on GPS Spoofing.

B. Images

This section contains higher-resolution versions of the main images in this report.

Flight Crew Survey Results



“ This is a **GPS Spoofing** survey for **Flight Crew** and Aircraft Operators.

Your answers will help the Workgroup to better understand how GPS Spoofing impacts aircraft and flight crew. We will complete our work by the end of August 2024, and can send you the final report.

The survey will take **5-7 minutes**.

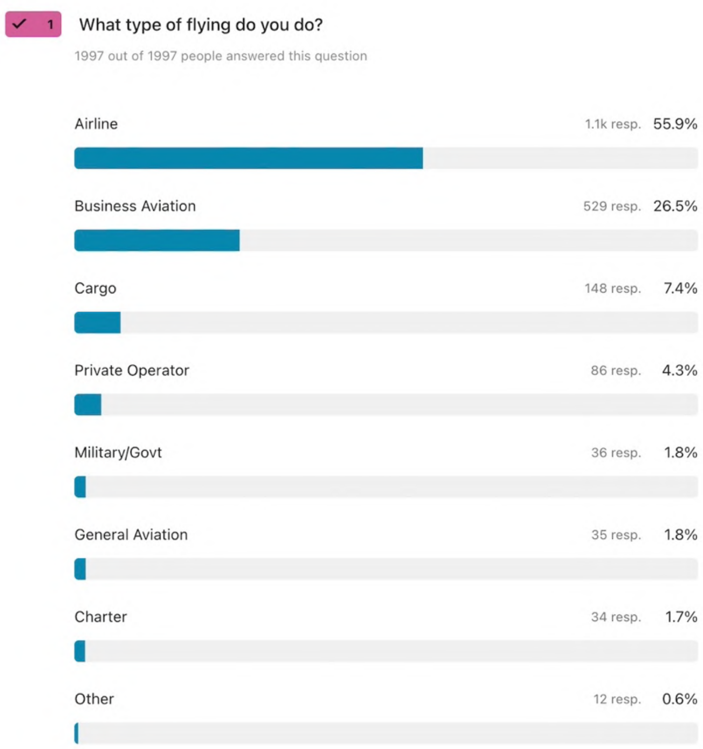
All answers are anonymous and de-identified. Thank you for helping!

During the WorkGroup, a Flight Crew Survey was created. Almost 2,000 responses were received, primarily from airline and business aviation pilots.

The most useful part of the survey responses was the flight crew feedback on mitigations, experiences, and suggestions, as well as supplied images, material, and data. This formed a great deal of the input to the Workgroup.

Below are the results.

Q1: Type of Flight Operation

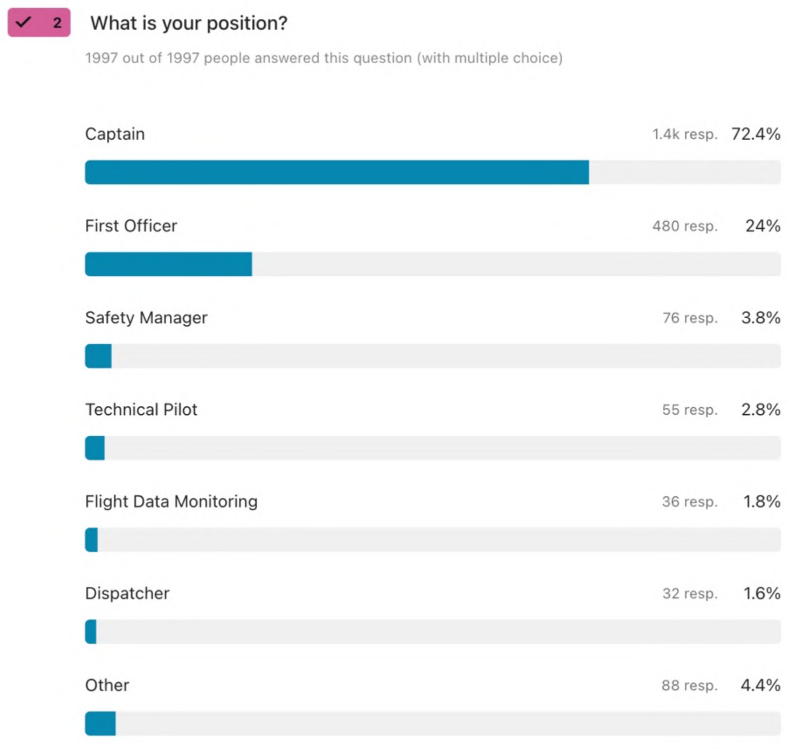


✓ 1 What type of flying do you do?

1997 out of 1997 people answered this question

- 56% of respondants were Airline
- 26% were Business Aviation
- 7% were Cargo
- 4% worked for a Private operator.

Q2: Position



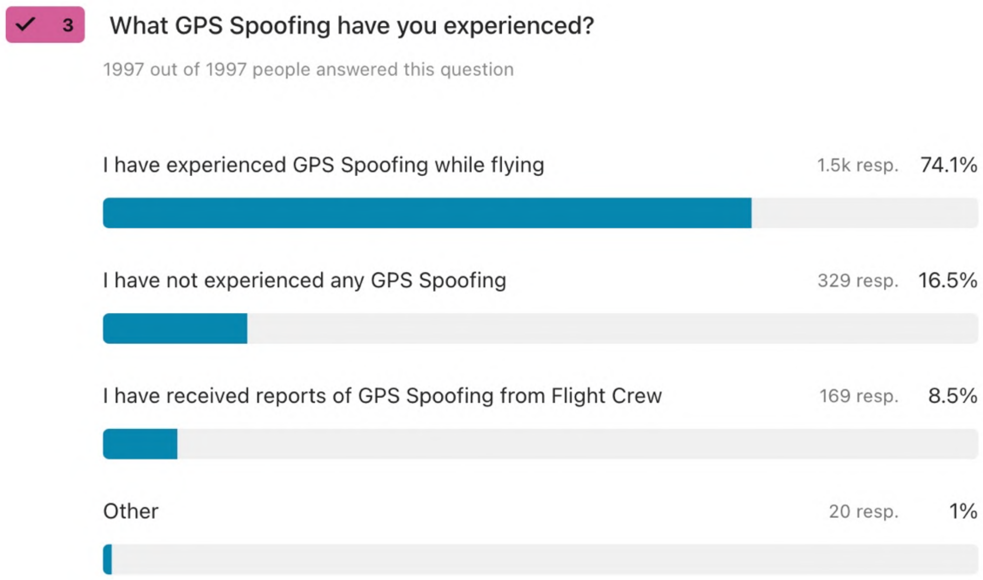
✓ 2 What is your position?

1997 out of 1997 people answered this question (with multiple choice)

Captain	1.4k resp.	72.4%
First Officer	480 resp.	24%
Safety Manager	76 resp.	3.8%
Technical Pilot	55 resp.	2.8%
Flight Data Monitoring	36 resp.	1.8%
Dispatcher	32 resp.	1.6%
Other	88 resp.	4.4%

- Multiple selections allowed
- 96% were pilots

Q3: What GPS Spoofing have you experienced?



✓ 3 What GPS Spoofing have you experienced?

1997 out of 1997 people answered this question

I have experienced GPS Spoofing while flying 1.5k resp. 74.1%

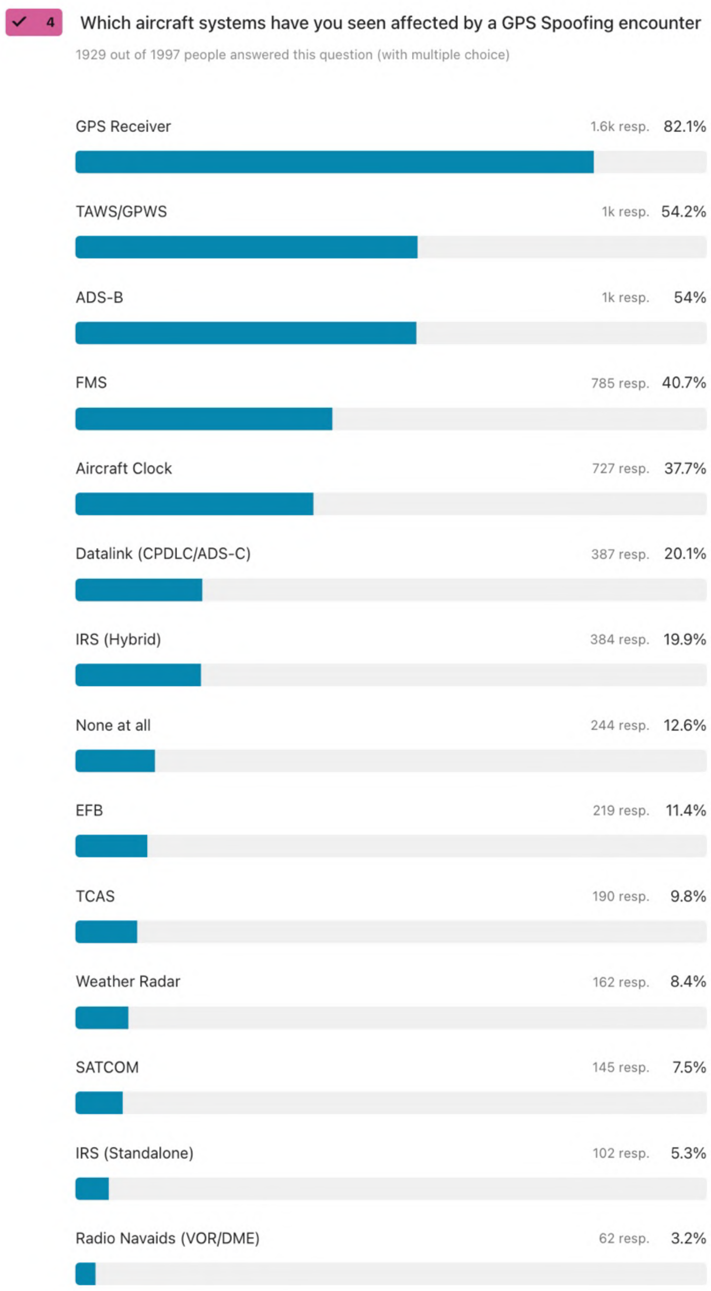
I have not experienced any GPS Spoofing 329 resp. 16.5%

I have received reports of GPS Spoofing from Flight Crew 169 resp. 8.5%

Other 20 resp. 1%

- 74% of respondants (1500 people) had experienced GPS Spoofing
- 8% had received reports of GPS Spoofing (e.g. Safety Manger, FDM)
- In total 84% of respondants had experienced or dealt with GPS Spoofing
- This doesn't mean that 74% of flight crew have experienced spoofing, it serves only to validate the opinions and experiences later in the survey.

Q4: Which aircraft systems have you seen affected?

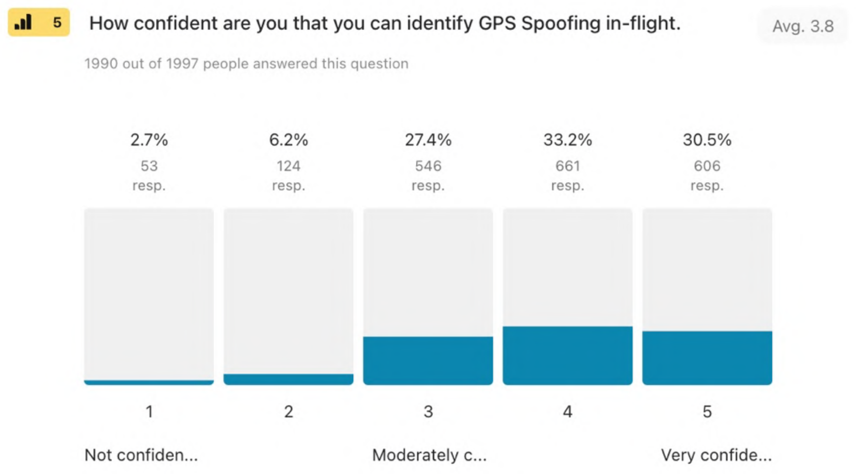


4 Which aircraft systems have you seen affected by a GPS Spoofing encounter

1929 out of 1997 people answered this question (with multiple choice)

- Multiple selections allowed
- TCAS response is more likely related to false ADS-B-in targets
- Other responses included: IRS INIT while on the ground, Fuel System (Automated Transfer), Frozen ND, Wind on ND, Backup speed scale (A321), SVS, EFVS, Wi-Fi, Internet, BTV, ROW / ROP, ANF, Airport Moving Map, Network File Server failure due to expired certificates.
- None of these are verified, but helped the group to identify systems to review.

Q5: How confident are you that you can identify GPS Spoofing in-flight?

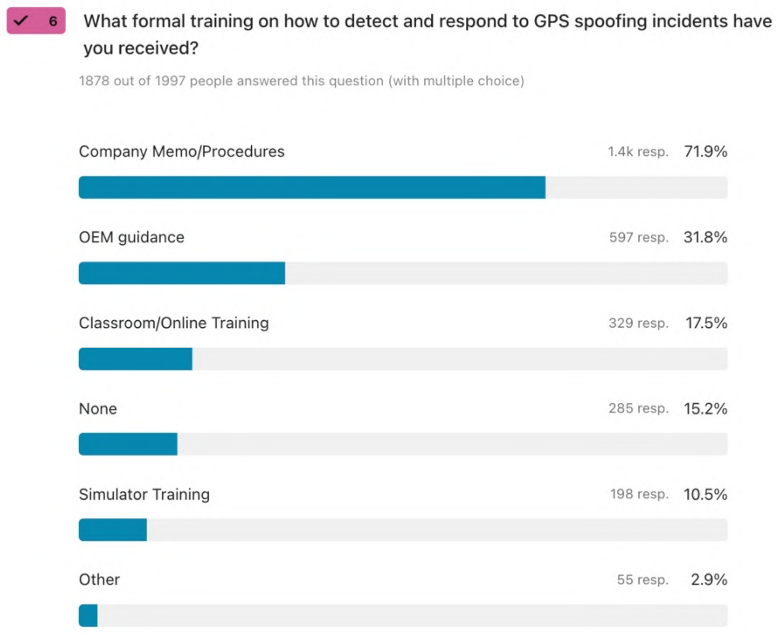


5 How confident are you that you can identify GPS Spoofing in-flight.

Avg. 3.8

1990 out of 1997 people answered this question

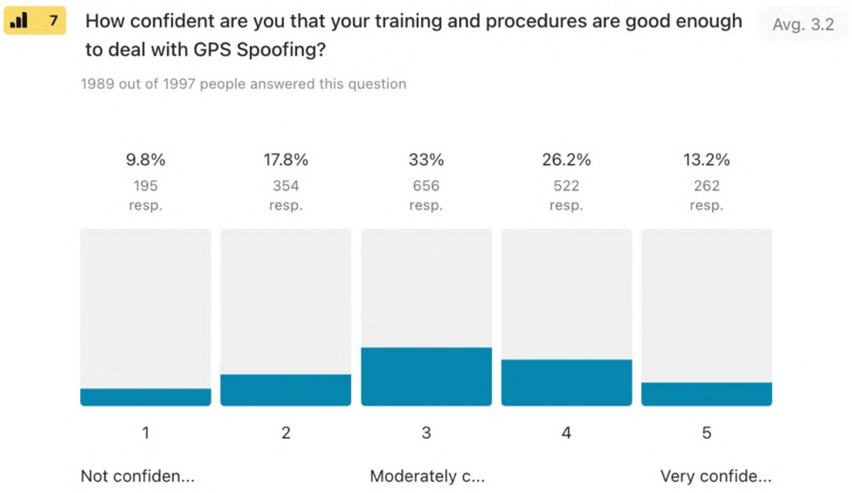
Q6: Formal Training on GPS Spoofing



6 What formal training on how to detect and respond to GPS spoofing incidents have you received?

1878 out of 1997 people answered this question (with multiple choice)

Q7: Confidence in training and procedures

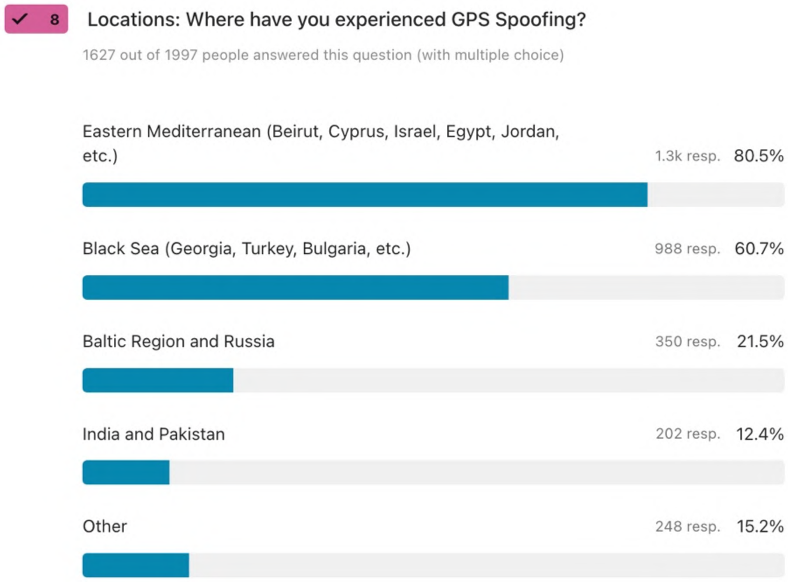


7 How confident are you that your training and procedures are good enough to deal with GPS Spoofing?

Avg. 3.2

1989 out of 1997 people answered this question

Q8: GPS Spoofing Locations

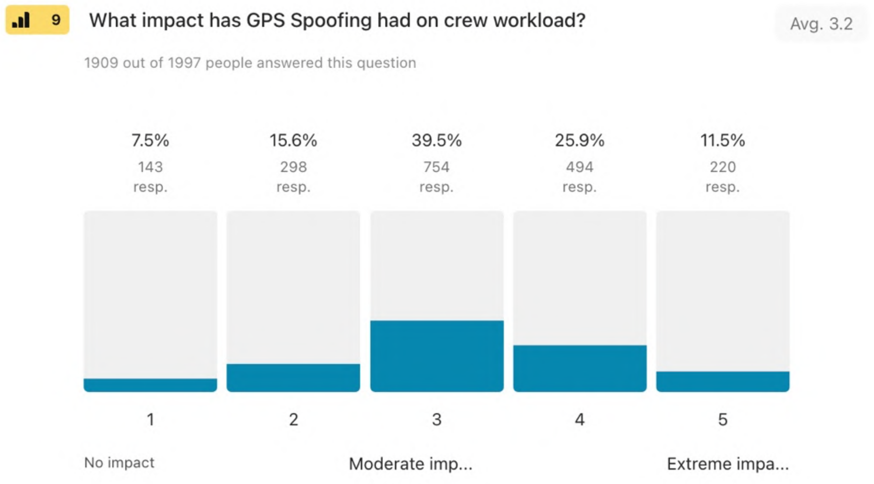


8 Locations: Where have you experienced GPS Spoofing?

1627 out of 1997 people answered this question (with multiple choice)

- Locations correlate strongly to data shown earlier in this report, under the Technical (Locations) section.

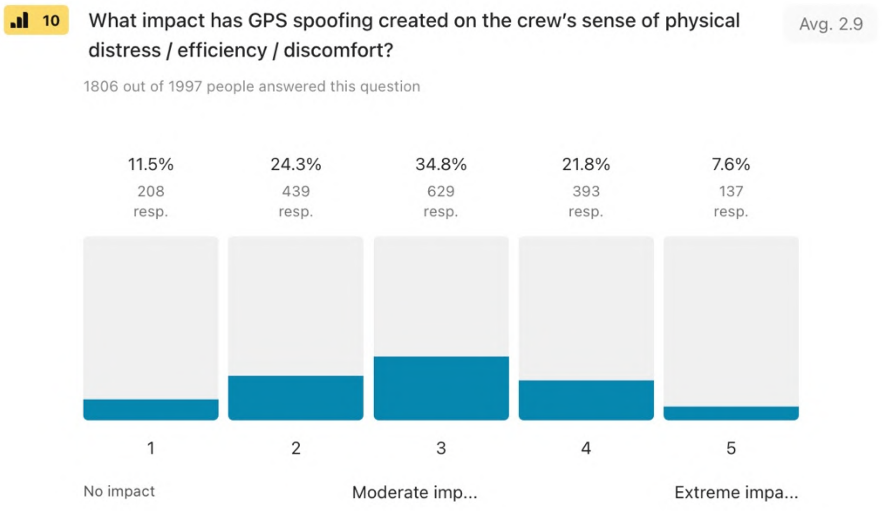
Q9 & 10: Workload and Crew Discomfort



9 What impact has GPS Spoofing had on crew workload?

Avg. 3.2

1909 out of 1997 people answered this question



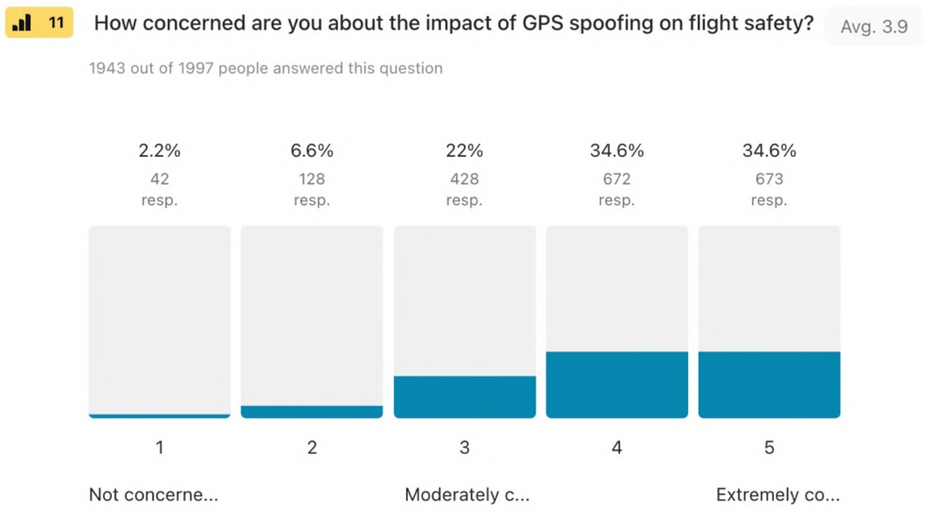
10 What impact has GPS spoofing created on the crew's sense of physical distress / efficiency / discomfort?

Avg. 2.9

1806 out of 1997 people answered this question

- 77% of crew reported a **moderate or greater** impact on crew workload
- 64% of crew reported a **moderate or greater** impact on their sense of physical discomfort.

Q11: Pilot view on Flight Safety



11 How concerned are you about the impact of GPS spoofing on flight safety? Avg. 3.9

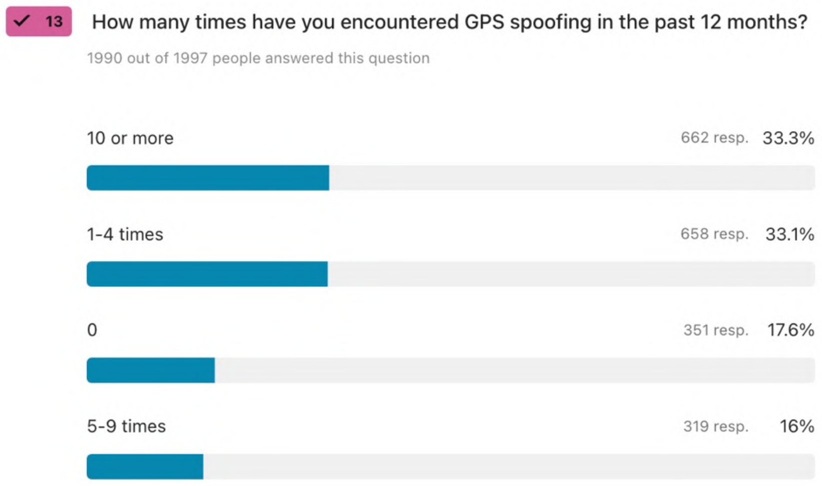
1943 out of 1997 people answered this question

- 69% of crew reported a **very high or extreme** concern about the impact of GPS spoofing on flight safety.
- 91% of crew reported a **moderate or greater** concern about the impact of GPS spoofing on flight safety.
- The WorkGroup found this the most concerning statistic from the survey.

Q12: Have you ended up in any unsafe situations as a result of GPS Spoofing?

- The results of this question are not shared, but have been reviewed by the WorkGroup and inform the Safety Concerns section.

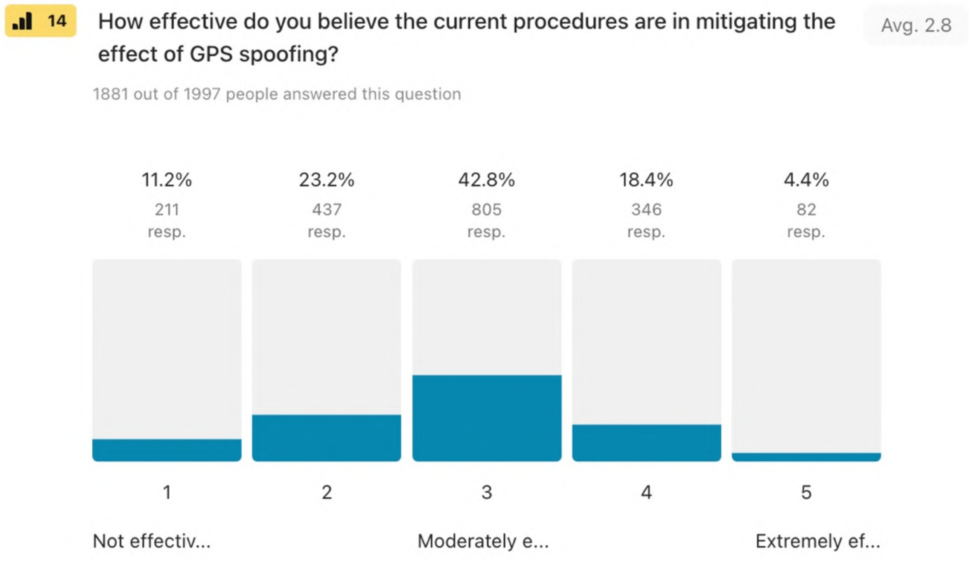
Q13: How many times have you encountered GPS spoofing in the past 12 months?



13 How many times have you encountered GPS spoofing in the past 12 months?

1990 out of 1997 people answered this question

Q14: How effective do you believe the current procedures are in mitigating the effect of GPS spoofing?

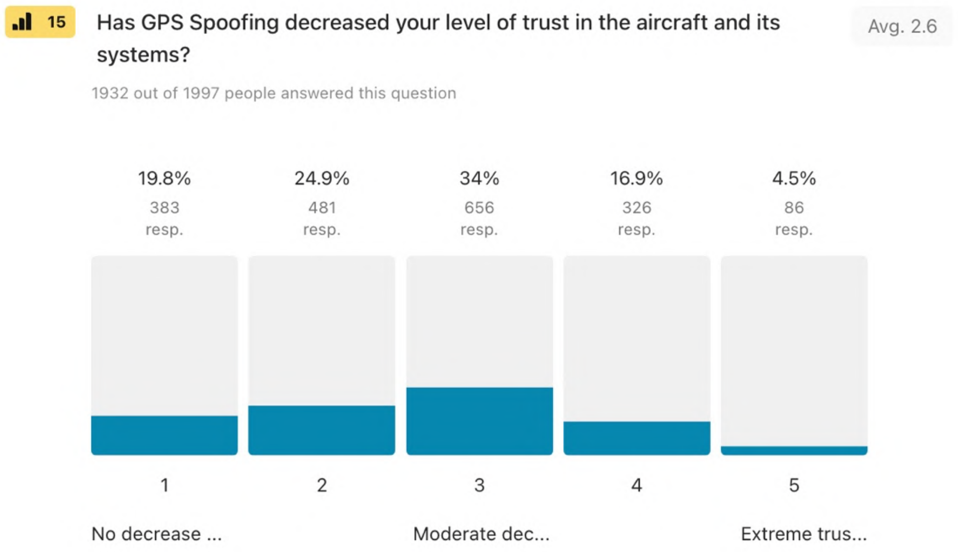


14 How effective do you believe the current procedures are in mitigating the effect of GPS spoofing?

Avg. 2.8

1881 out of 1997 people answered this question

Q15: Has GPS Spoofing decreased your level of trust in the aircraft and its systems?

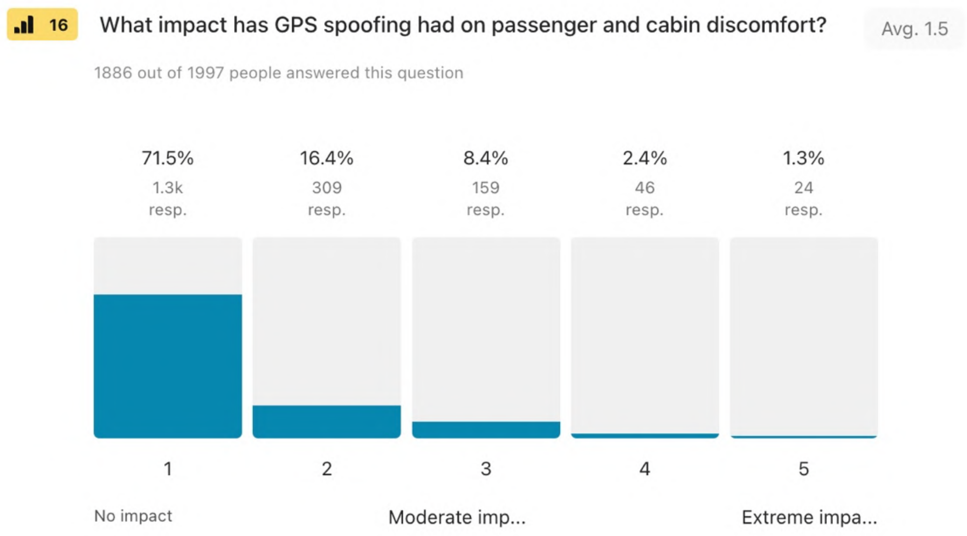


15 Has GPS Spoofing decreased your level of trust in the aircraft and its systems?

Avg. 2.6

1932 out of 1997 people answered this question

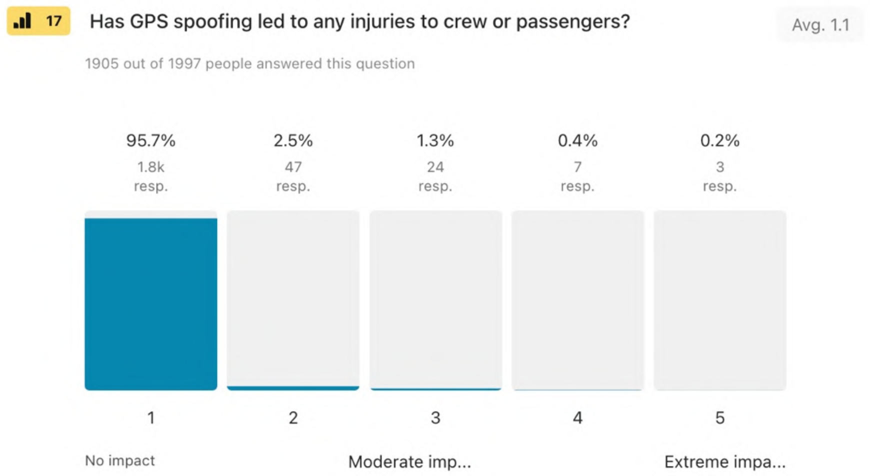
Q16 & 17: Passenger & Cabin Comfort



16 What impact has GPS spoofing had on passenger and cabin discomfort?

Avg. 1.5

1886 out of 1997 people answered this question



17 Has GPS spoofing led to any injuries to crew or passengers?

Avg. 1.1

1905 out of 1997 people answered this question

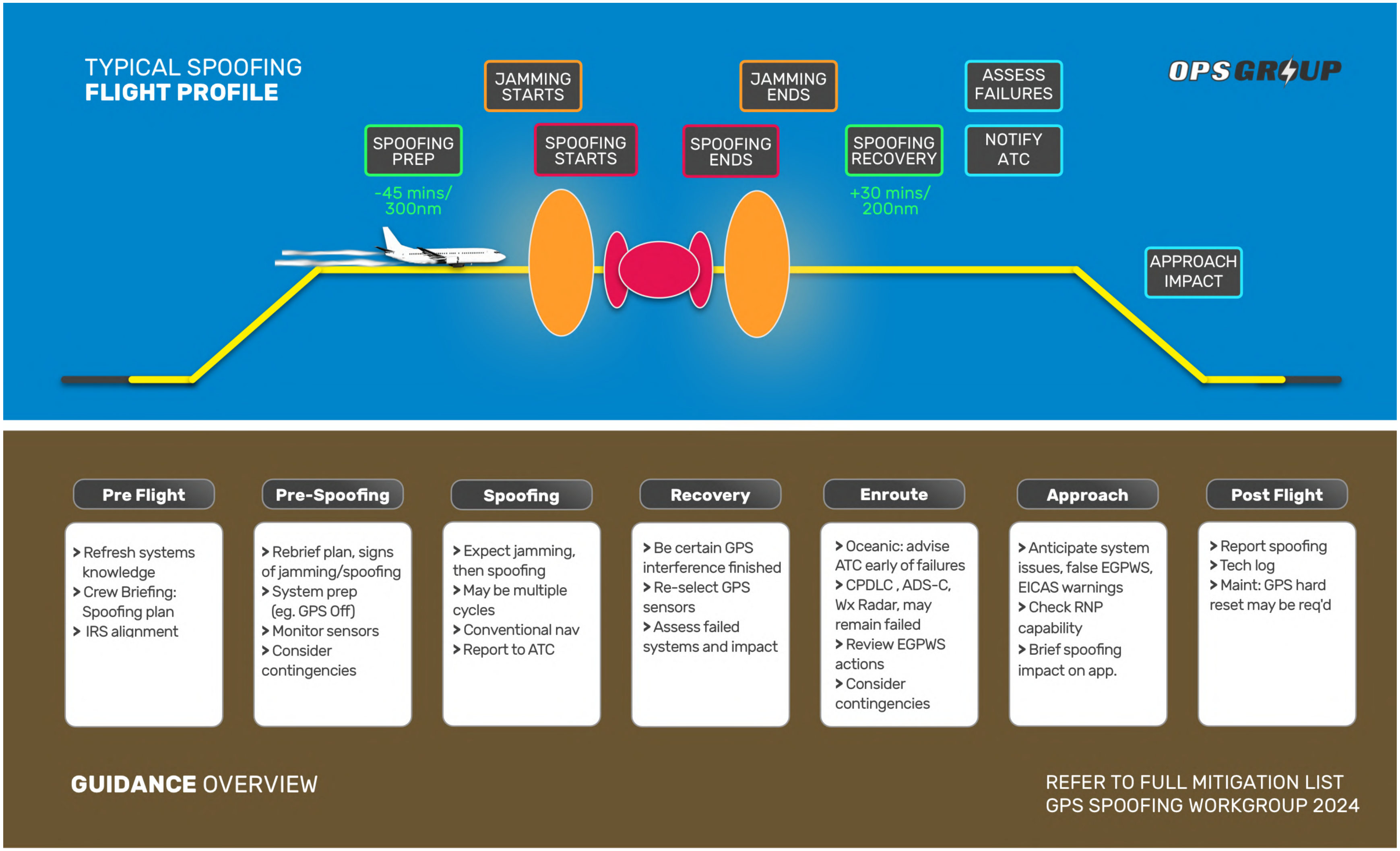
Q18: What mitigation techniques have been most effective to combat the effects of GPS Spoofing?

- The results of this question are not shared, but have been reviewed by the WorkGroup and inform the Safety Concerns section.

Q19: Freeform report - share any additional comments or thoughts

- The results of this question are not shared, but have been reviewed by the WorkGroup and inform the Safety Concerns section.

Figure 1 Typical Spoofing Flight Profile



Pre Flight

- Refresh systems knowledge
- Crew Briefing: Spoofing plan
- IRS alignment

Pre-Spoofing

- Rebrief plan, signs of jamming/spoofing
- System prep (eg. GPS Off)
- Monitor sensors
- Consider contingencies

Spoofing

- Expect jamming, then spoofing
- May be multiple cycles
- Conventional nav
- Report to ATC

Recovery

- Be certain GPS interference finished
- Re-select GPS sensors
- Assess failed systems and impact

Enroute

- Oceanic: advise ATC early of failures
- CPDLC , ADS-C, Wx Radar, may remain failed
- Review EGPWS actions
- Consider contingencies

Approach

- Anticipate system issues, false EGPWS, EICAS warnings
- Check RNP capability
- Brief spoofing impact on app.

Post Flight

- Report spoofing
- Tech log
- Maint: GPS hard reset may be req'd

GUIDANCE OVERVIEW

REFER TO FULL MITIGATION LIST
GPS SPOOFING WORKGROUP 2024

Figure 2 GPS Reception – Normal, Jamming, Spoofing

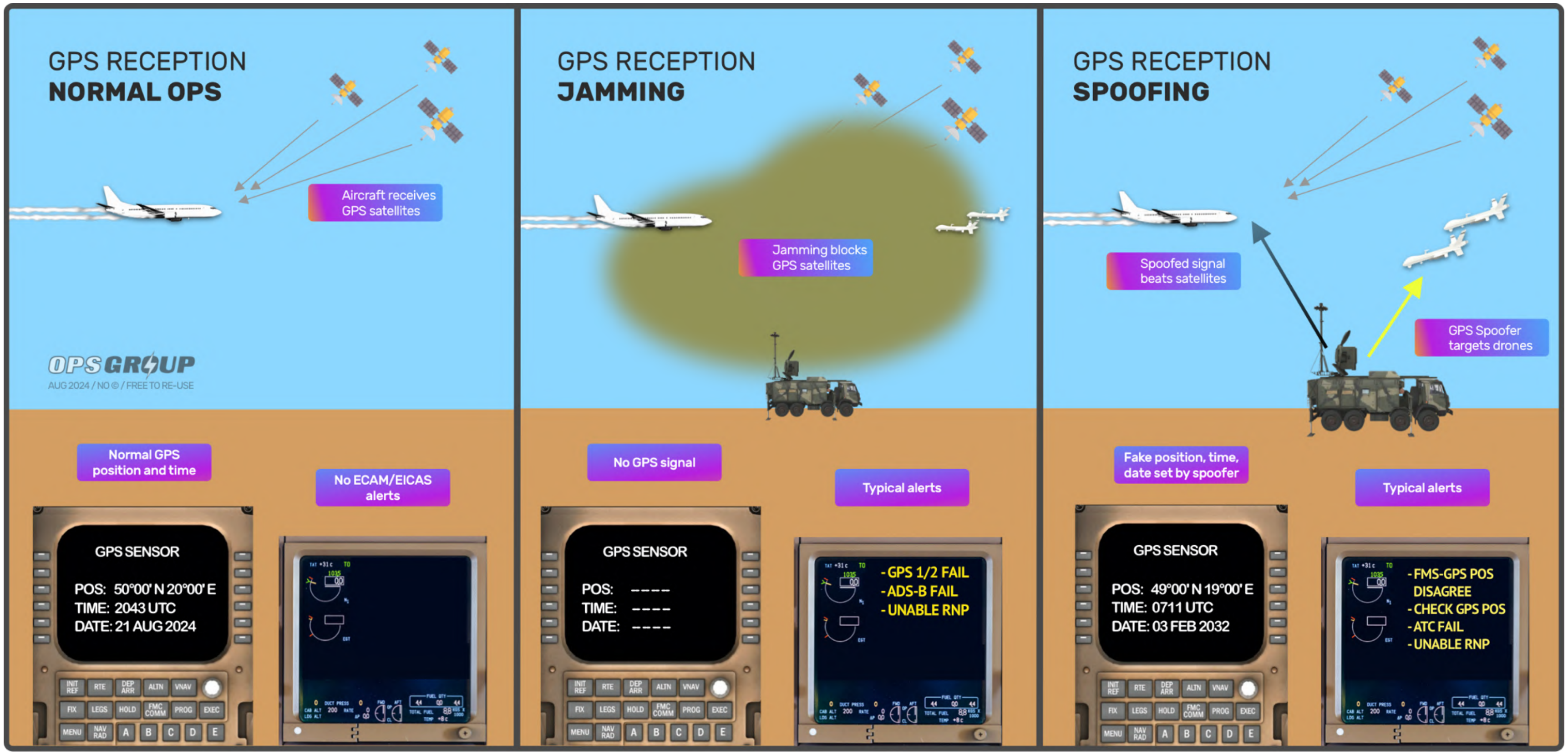
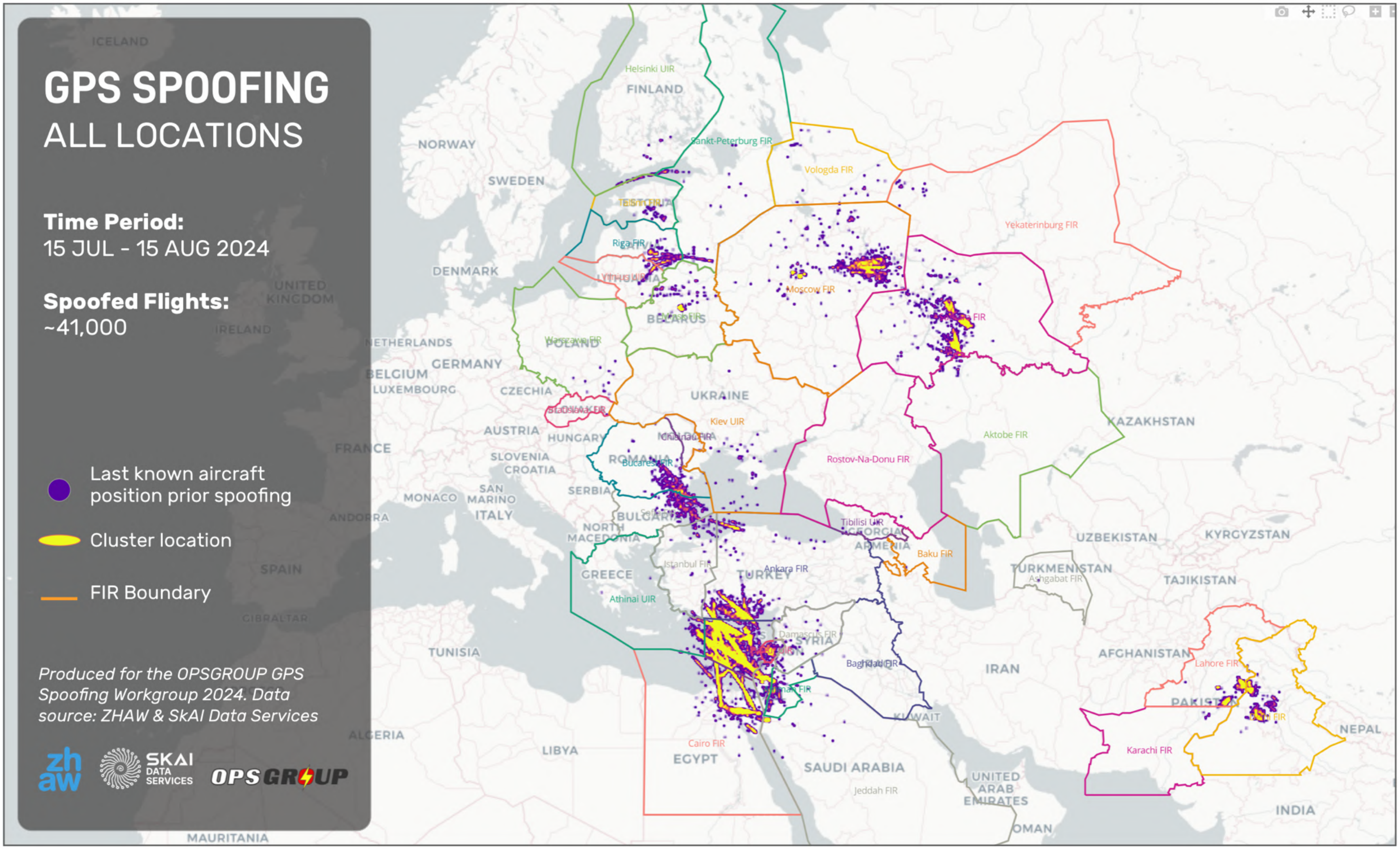


Figure 3 GPS Spoofing Location Map – Worldwide



Produced for the OPSGROUP GPS Spoofing Workgroup 2024. Data source: ZHAW & SkAI Data Services

Figure 4 GPS Spoofing Location Map – Eastern Mediterranean

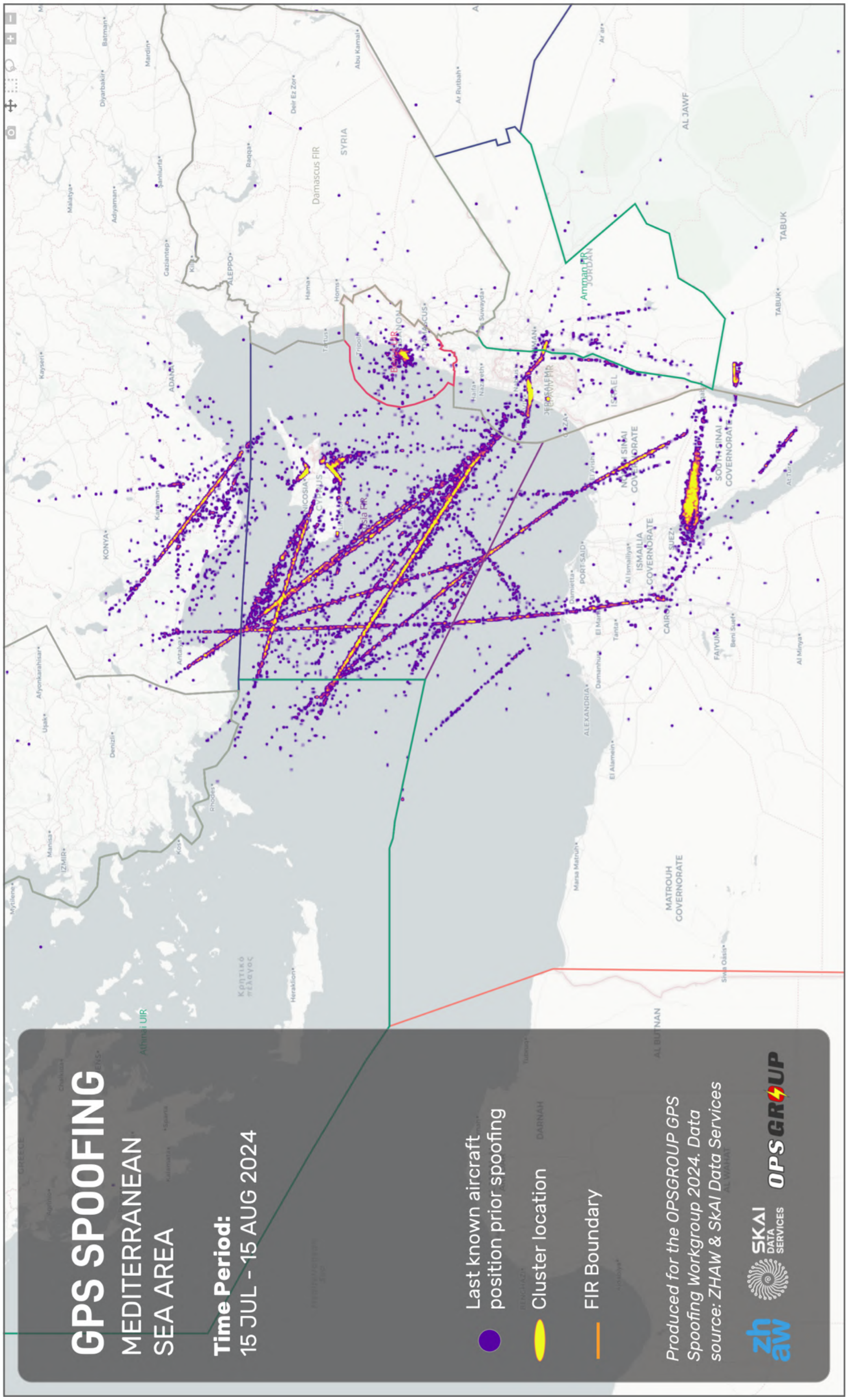
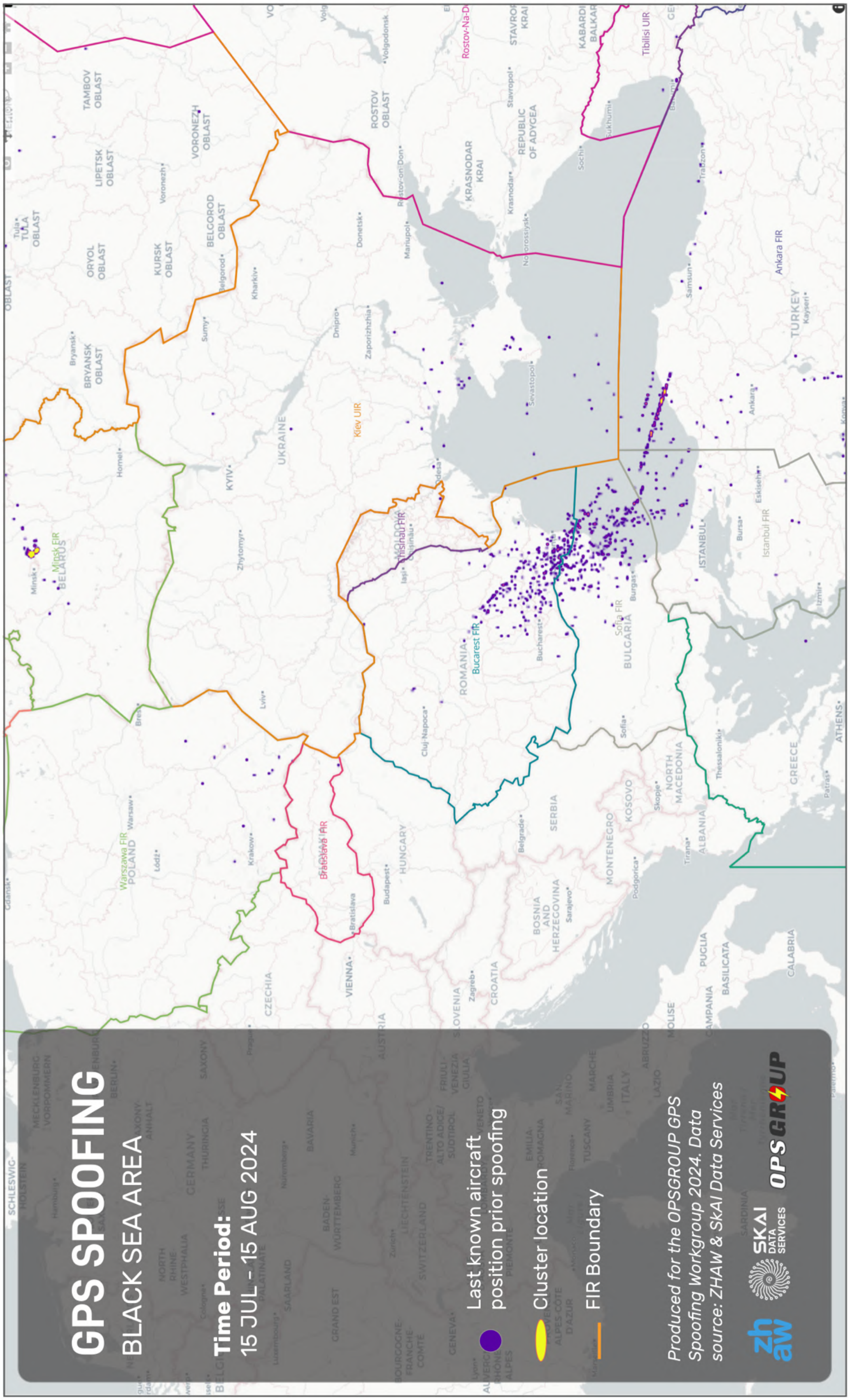


Figure 5 GPS Spoofing Location Map – Black Sea



GPS SPOOFING

BLACK SEA AREA

Time Period: 15 JUL - 15 AUG 2024

● Last known aircraft position prior spoofing

● Cluster location

— FIR Boundary

Produced for the OPSGROUP GPS Spoofing Workgroup 2024. Data source: ZHAW & SKAI Data Services

Figure 6 GPS Spoofing Location Map – Russia & Baltic Area

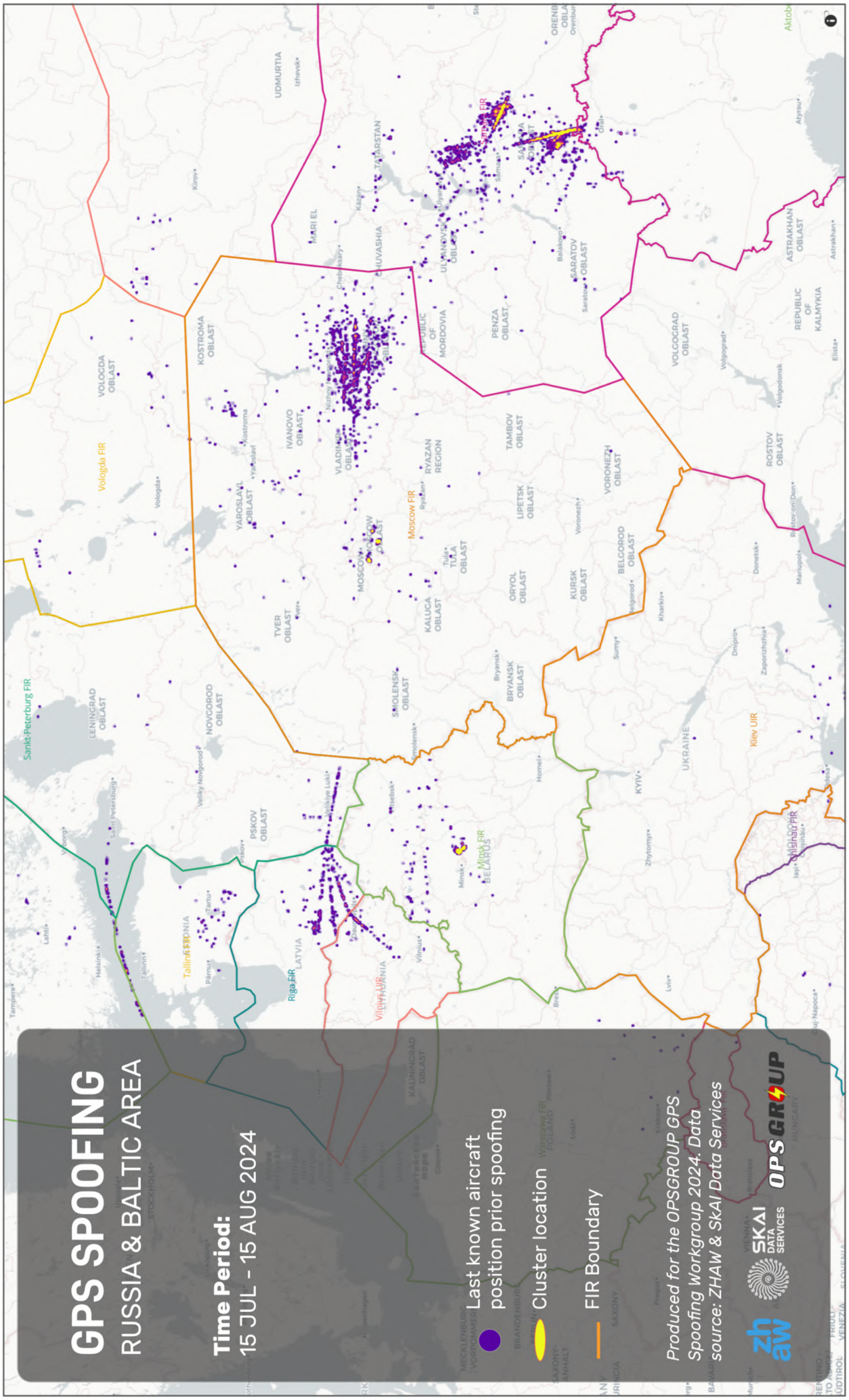
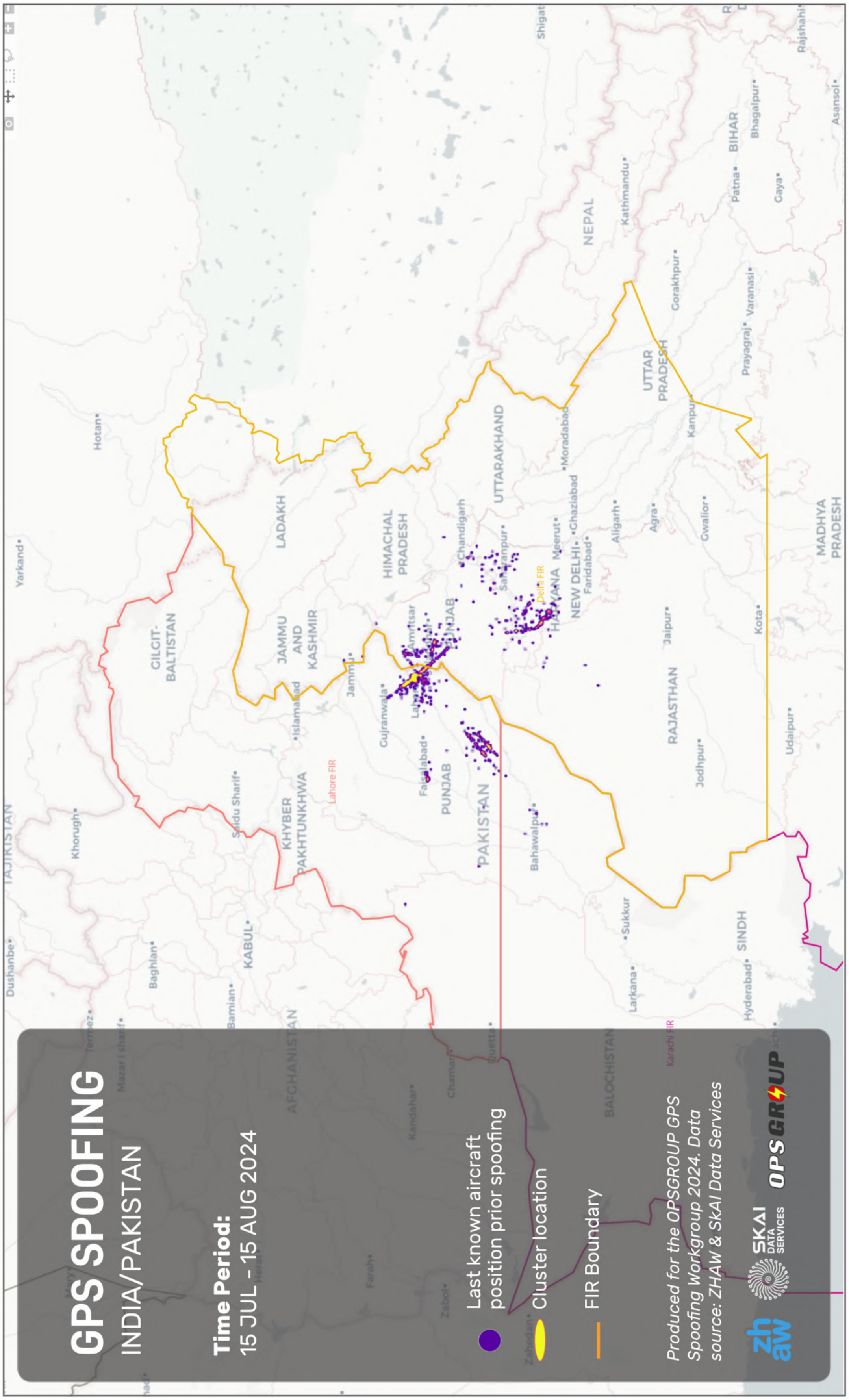
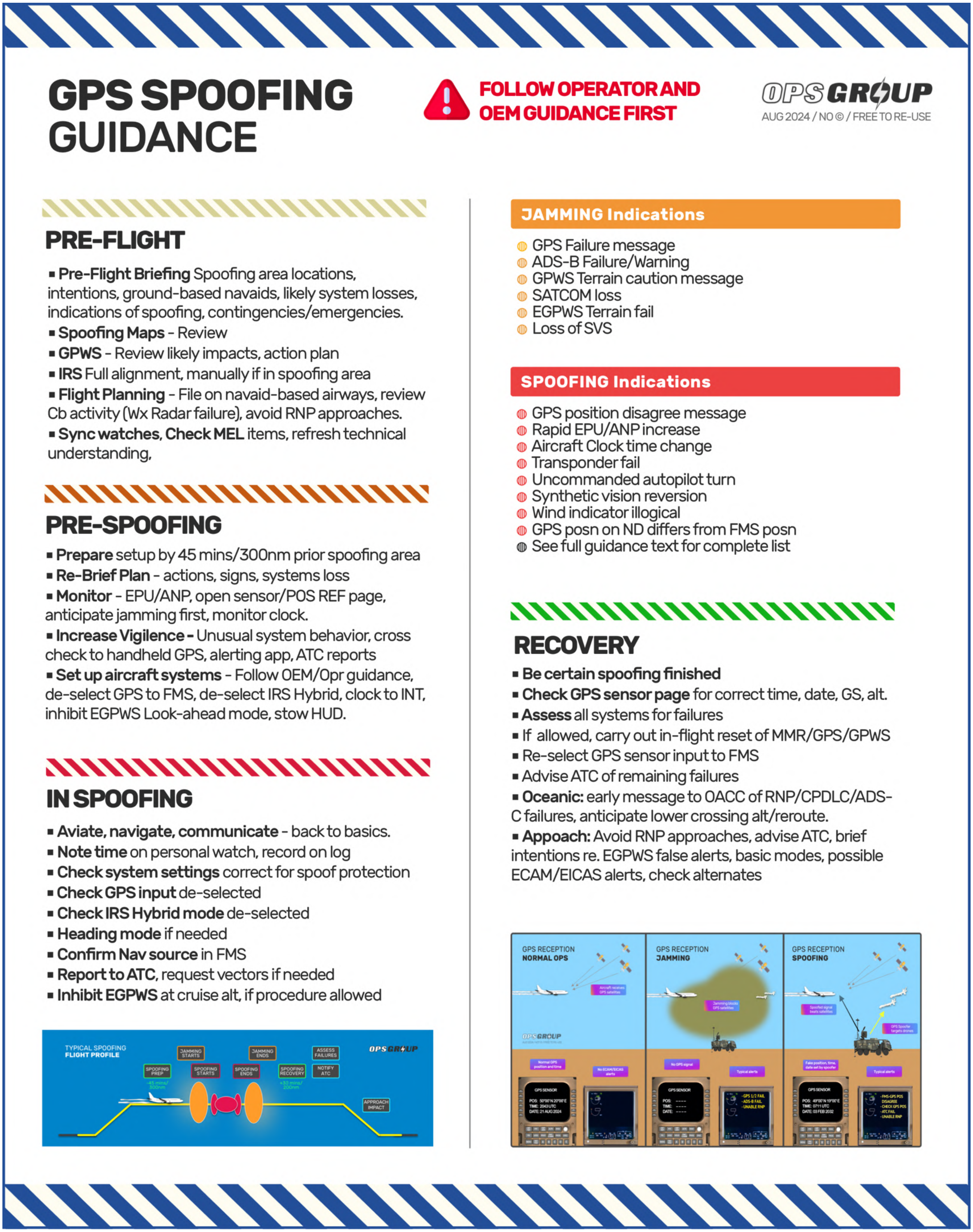


Figure 7 GPS Spoofing Location Map – India/Pakistan



Produced for the OPSGROUP GPS Spoofing Workgroup 2024. Data source: ZHAW & SKAI Data Services

Figure 8 Crew Guidance one-page summary



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