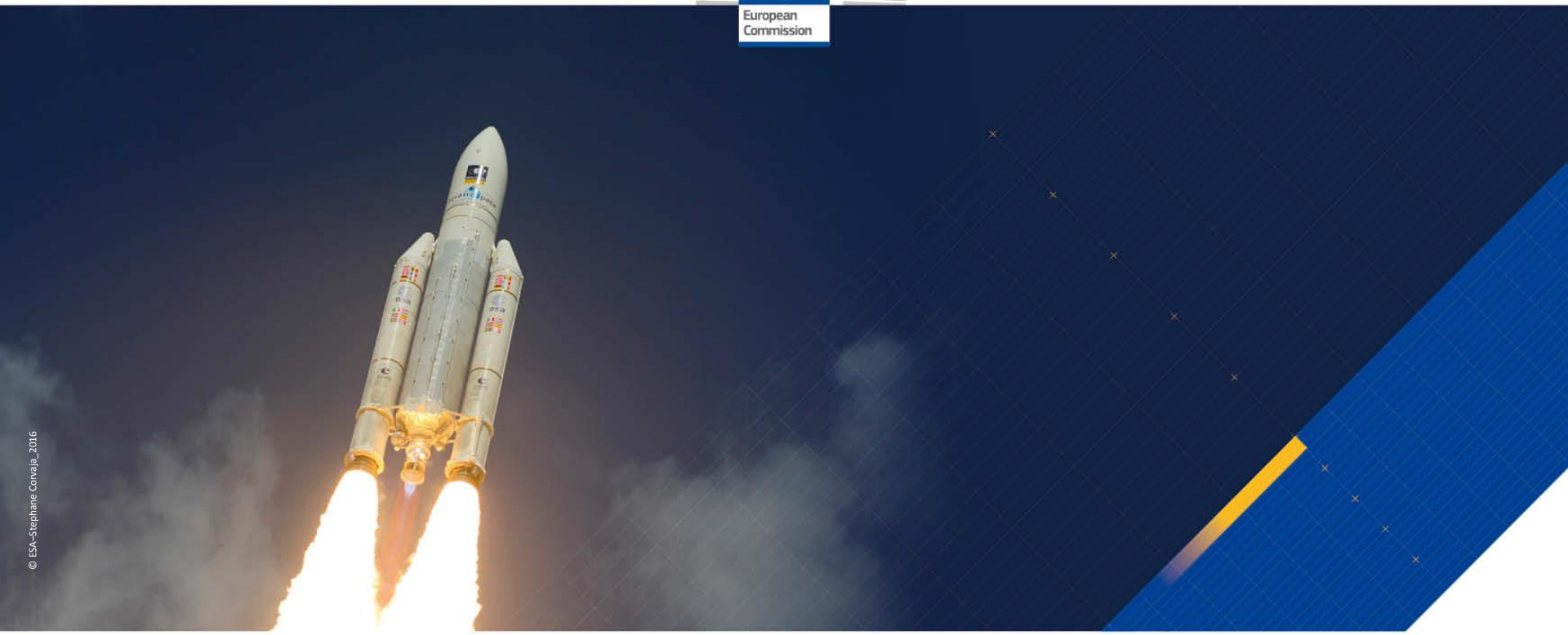


EU *Protect, Toughen, Augment* Activities

PNT Advisory Board • Redondo Beach • 5/6 December 2018

Dominic HAYES • European Commission

THE PROBLEM

CULTURE

Truck driver has GPS jammer, accidentally jams Newark airport

An engineering firm worker in New Jersey has a GPS jammer so his bosses don't know where he is all the time. However, his route takes him close to Newark airport, and his jammer affects its satellite systems.

BY **CHRIS MATYSZCZYK** / AUGUST 11, 2013 8:08 AM PDT

THE PROBLEM

CULTURE

Truck driver has GPS jammer, accidentally jams Newark airport

Russia has figured out how to jam U.S. drones in Syria, officials say

Four U.S. officials said Russia's signal scrambling has seriously affected military operations.

by Courtney Kube / Apr.10.2018 / 10:32 AM GMT+2 / Updated Apr.10.2018 / 5:16 PM GMT+2

THE PROBLEM

CULTURE

Truck driver has GPS jammer, accidentally jams Newark airport

Russia has figured out how to jam U.S. drones in Syria, officials say

Four U.S. officials said Russia's signal scrambling has seriously affected military

Russian military training along the border. Photo: Mil.ru

Norway requests Russia to halt GPS jamming in borderland

Intensive military training on the Russian side of the border creates increasing communications troubles for nearby Norwegians.

By **Atle Staalesen**

April 27, 2018

THE PROBLEM

CULTURE

Incident: France A319 at Munich on Jul 14th 2018, loss of positioning system

By Simon Hradecky, created Saturday, Jul 14th 2018 21:08Z, last updated Saturday, Jul 14th 2018 21:08Z

An Air France Airbus A319-100, registration F-GRHB performing flight AF-1123 from Munich (Germany) to Paris Charles de Gaulle (France), was in the initial climb out of Munich's runway 26L when the crew reported they had lost their positioning system, they were maintaining runway heading and needed radar vectors to return to Munich. The aircraft stopped the climb at 5000 feet, was vectored for the approach and landed safely back on runway 26L about 20 minutes after departure.

According to information The Aviation Herald received both GPS systems showed a fault.

The aircraft remained on the ground for about 2:45 hours, then was able to depart and reached Paris with a delay of 3.5 hours.

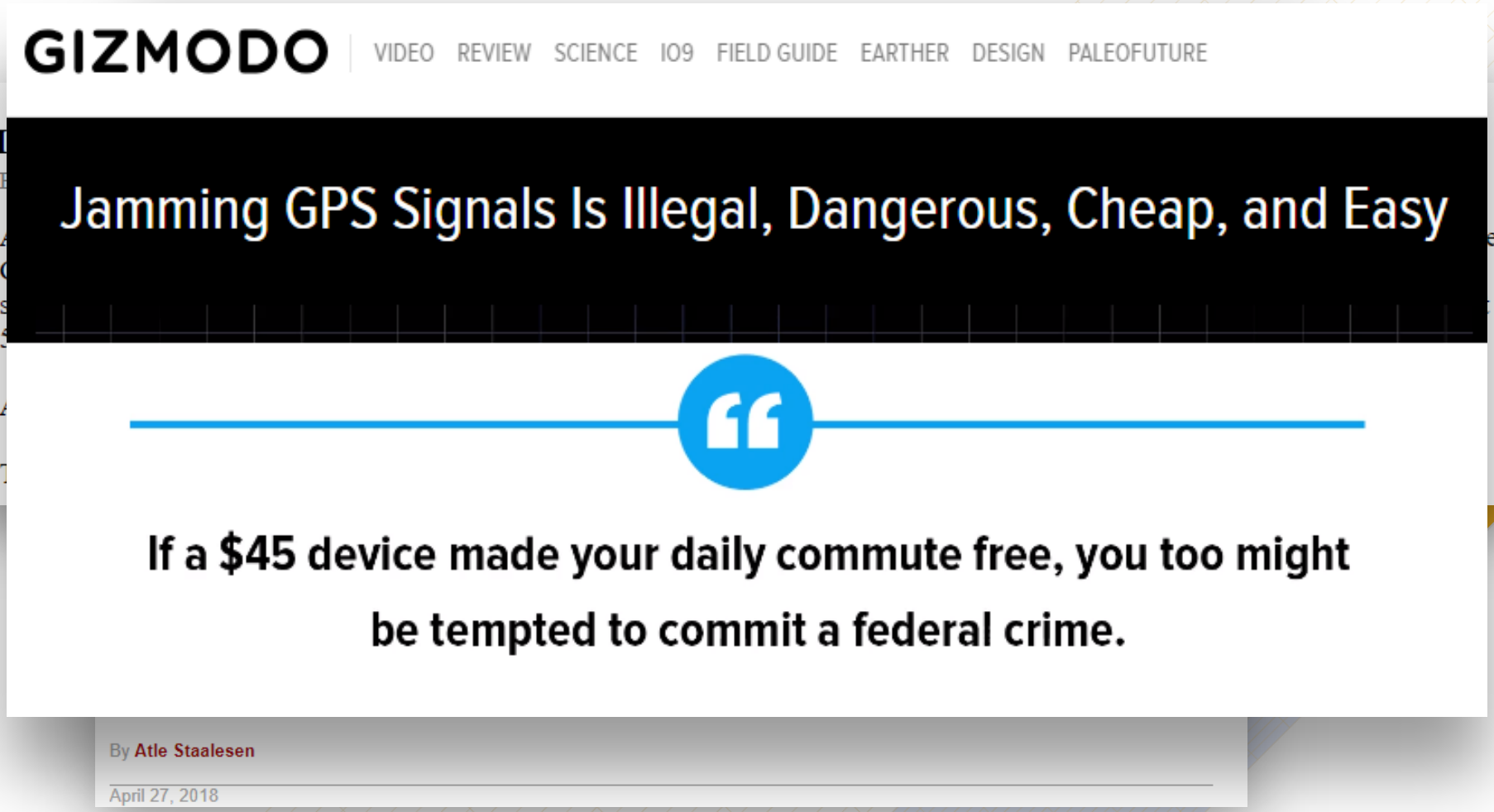
Norway requests Russia to halt GPS jamming in borderland

Intensive military training on the Russian side of the border creates increasing communications troubles for nearby Norwegians.

By Atle Staalesen

April 27, 2018

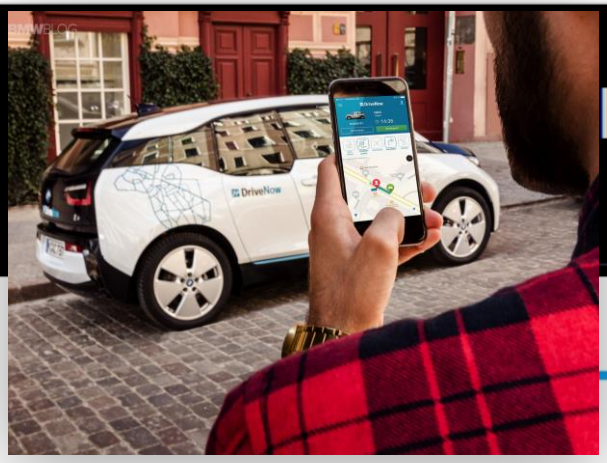
THE PROBLEM


GIZMODO
VIDEO REVIEW SCIENCE IO9 FIELD GUIDE EARTHER DESIGN PALEOFUTURE
Jamming GPS Signals Is Illegal, Dangerous, Cheap, and Easy
If a $45 device made your daily commute free, you too might be tempted to commit a federal crime.
By Atle Staalesen
April 27, 2018

THE PROBLEM

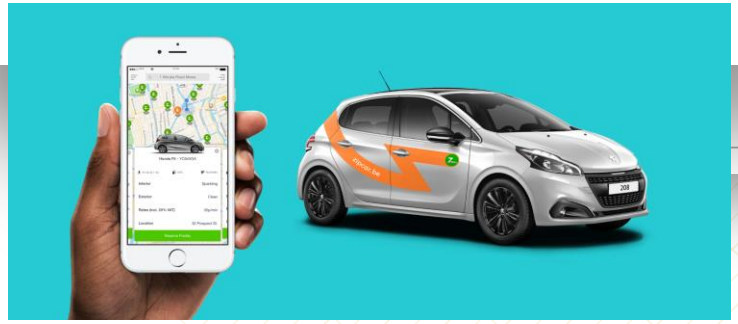
GALILEO EGNOS
NAVIGATION SOLUTIONS
POWERED BY EUROPE

GIZMODO | VIDEO REVIEW SCIENCE IO9 FIELD GUIDE EARTHER DES



Is Is Illegal, Dangerou asy

If a $45 device made your daily commute fr
be tempted to commit a federal



SPOOFING VS JAMMING

Spoofing – fools GNSS receiver into thinking it's somewhere else

- technically more challenging
- typically only by security/military, sensitive in nature
- However, there are signs that this will become more of an issue sooner than anticipated, the 'Pokémon GO effect'
  - ➢ GALILEO's OS NMA and CS Authentication should help mitigate this kind of challenge
- EU Member States consider to be a more sensitive issue

Jamming – easy

- Discrete plug-in jamming devices available for a few euros
- Can be crudely constructed with relatively simple equipment

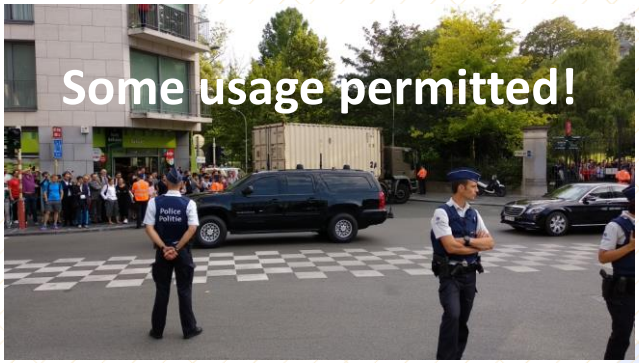
JAMMING

- Jamming is easy because GNSS signals received on Earth are very low powered – below the ‘background noise level’
- ‘Low powered’ jammers (5mW) can disrupt over 10-100m
- Already seeing proliferation of such personal jamming devices
- Time consuming to detect these using traditional “direction finding” techniques
- Novel techniques are required to detect and identify such low-powered jammers

- Higher powered jammers 1W+ can disrupt over 1 to 100+ km range, but are consequently easier to detect and localise. Typically used for military applications

PROTECT

LEGAL MATTERS



- The act of jamming is illegal.
  - 'Illegal' under ITU Radio Regulations
  - 'Illegal' under CEPT rules
  - Illegal under EU laws
    - EU's Radio Equipment Directive and EMC Directive
  - Illegal under national laws (implemented EU regulations)
    - Uncertainty about whether EU regulations have indeed been implemented uniformly across all MS
- The import and sale of jamming devices is illegal at EU level
- The ownership of jamming devices is not always illegal, depends on the country concerned

WHO DOES WHAT?

National regulators and Agencies:

- Ultimately **responsible** for spectrum
- Different countries do things in different ways
- Scope for sharing best practice on general spectrum protection already done in CEPT (European 'ITU'), but GNSS needs a **focussed** activity
- Work at international level, CEPT, ITU, IMO

At **EU level**, the EC :

- can help to **coordinate** activities
- Bring together expertise
- Provide **funding** for projects
- Interact at **international** level, eg ICG, ITU, CEPT, IMO

WHAT IS BEING DONE?

At **European** level

- GSA's PROTECTOR, DETECTOR and STRIKE3 projects
- Related, ESA Interference Monitoring System study
- Eurocontrol interference logging activities

At **CEPT** level

- French initiative in WG FM

At UN **International** Committee for GNSS (ICG)

- EC is working with the other providers on interference detection and mitigation (IDM) and promotion/outreach efforts to keep spectrum clean
- Crowdsourcing is thought to be a promising approach, but privacy data issues are huge challenge

EU FUNDED PROJECTS

- **PROTECTOR (2009 – study)**
  - Definition of the means needed to protect the European GNSS systems and services against radio-sources interferences to prevent service disruptions. The study examined the risks and proposed a Jamming and Interference Monitoring System concept and explores how JIMS can interface with MS and with the European GNSS Security Centre.
  - Status: completed

- **DETECTOR (FP7 – total cost 0,75 Me))**
  - Development of a low-cost GNSS radio frequency interference detection service for use within road transport and critical applications.
  - Partners: NSL, SANEF, ARIC, Univ. Bologna, Black holes, JRC,
  - Status: completed

- **STRIKE3 (H2020 – total cost: 1,3 M€))**
  - aims at standardising the systems, processes and interfaces for GNSS interference reporting and receiver testing
  - Partners: NSL, FOI, NLS, ARIC, Catapult, GNSS Labs, ETRI
  - Status: on-going – test installations across the globe, US interest?

CROWDSOURCING CHALLENGES

- Crowdsourcing relies on shared data
- Personal data, such as location is intrinsically private
- EU data laws are **strong** – for good reason
- Therefore sharing of location (and signal data) requires explicit **opt-in**
- Achieving sufficient critical mass of useful data may therefore be a challenge
- A **proof of concept**, test system could potentially identify a professional group that may see benefit in participating, blue light services, taxi, delivery – EC plans to investigate
- Output would be useful to regulators for follow-up actions

BRINGING EU ACTIVITIES TOGETHER

- Existing technical groups dealing with frequencies and signals not sufficient to handle
  - ➢ the jammers challenge cuts across domains, strategy, policy, legal, communication and technical

Therefore:

- Needs a dedicated "**task force**" to evaluate and recommend options
- MS still regard this as a sensitive issue, so any task force should not touch topics of national prerogative

PROPOSED EU TASK FORCE

to evaluate and recommend options to the EC

- Would consider topics related to finding solutions in the domain of **policy**, **legal** and **communication**
- Composed of relevant experts from MS, GSA, ESA and other international organisations
- Chaired by the European Commission
- Consult expert EC groups, consider trial projects, liaise with other groups outside EC
- Sensitive to MS concerns, will not cover any topics related to security
- **Limited duration**, would report back EC programme managers
- ToR to be drafted and would need to be approved by MS

TASK FORCE OBJECTIVE

- The output of the task force would:
  - Provide an overview of current jammer usage affecting GNSS
  - Propose actions related to policy, legal, communication (e.g. awareness raising, identify forum to threat some actions)
- Output reviewed and presented to EC Programmes Committee
- The TF will specifically not address:
  - Matters related to PRS/military usage
  - inventory of threats and vulnerabilities posed by jammers and spoofers (neither from system nor user perspective)
  - Other aspects may be agreed with MS

TOUGHEN

ADDITIONAL EFFORT THAT MAY HELP

European Radio Navigaton Plan (ERNP)

- Inspired by the US Federal Radionagation Plan, takes a snapshot of the EU radionavigation capabilities
- Currently in V1.0, it will evolve, and help to identify gaps and vulnerabilities, with possible actions, ultimately helping to guide EU/MS strategies
- May help identify appropriate backup options to mitigate the effects of jamming

ACTIVITIES

- EC and GSA projects are considering technologies to improve **receiver robustness**
- EU working actively in EU/US working group on robust GNSS applications, eg for aviation
- Robust encrypted PRS signal could be used by Member States for critical infrastructure as national prerogative

AUGMENT

RESILIENCY

- EC has formed a working group on Resiliency
- Considering PNT backup options
  - already recognised: no single backup solution as different sectors have different needs
- Initial EC workshop October 2018
  - 1hr GNSS outage major impact on most sectors
  - 1day outage critical
- Further workshops expected as the working group progresses
- Still early days for this aspect at EU level, some MS have been working independantly

SCOPE TO IMPROVE

- Multiple actions are taking place at many levels across the globe
  - ➢ MS, EU, CEPT, ITU (rules), UN ICG, Eurocontrol/ICAO
- Disparate activities perhaps promote novel solutions…
- But ultimately the various activities should be better coordinated to share and pool knowledge and knowhow
- Communication – many people do not realise jamming is illegal or realise it is not personal

➢ **We can, and should, and will do better given the amount Europe is investing in EGNSS and the value to the EU economy**

Yesterday's transport disruptor:
easy to spot

Today's jammer:
not so easy

http://ec.europa.eu/galileo