# Redefining Criminality in the Age of Ubiquitous Satnav Technology

**Summary**

This paper/presentation explores the relatively new phenomena of the widespread and international use of GPS jammer technology and the way that this technology is used to disrupt Satnav technology. This emerging threat is pointing to a clear need to redefine criminality across a wide variety of use cases.

Through sales of GPS jamming detection technology to international police forces and counter terror/homeland security organisations, Chronos is in a unique position to share actual case study stories from the field.

This insight has led us to believe that Governments need to redefine criminality in the light of the increasing use of low cost jammer technology. These devices have now been found in satnav neutralisation applications such as young driver insurance, spoofing of smart tachos, fleet management and offender tracking applications as well as serious and organised crime activity such as drugs/narcotics distribution, truck hijacking, vehicle and asset theft and rival gang wars.

One example of the emerging dilemma is the recent seizure of a jammer from an 18-year-old driving with “young driver” insurance cover. What if he has a crash or injures someone? Is his insurance invalidated by the use of the jammer? This paper does not offer answers but is intended to raise awareness of the threat for relevant law enforcement organisations. The law is clearly different in each country and we do not intend to make recommendations; that is for relevant justice ministries to decide and formulate new laws based on the emerging facts.

**Background and Introduction**

GPS Jammers are now being regularly recovered by police officers using technology developed by Chronos Technology in partnership with the University of Bath and researched under various Innovate UK Grant supported collaborative research projects, notably GAARDIAN, SENTINEL and AJR. This technology was recognised by the Royal Institute of Navigation and awarded the Duke of Edinburgh Award for Technology at the RIN AGM in July 2018.

Police officers with Hampshire and Gloucestershire constabularies are equipped with two different types of hand-held jammer detectors CTL3510 and CTL3520 in their patrol cars and motorbikes. CTL3530 “JammerCam” trial systems are installed at Gloucester Services, Felixstowe Docks and Portsmouth Ferry Port. JammerCam can take a photo of a passing vehicle carrying a jammer

By the nature of jammer use and detection, real evidence and use-case scenarios are hard to come by. Working with police forces is informing the national law enforcement knowledge-base as well as taking jammers out of circulation.

The resulting jammer seizures and JammerCam photo-captures is informing and developing a growing knowledge of use-case scenarios. This paper reviews these use-case scenarios and quotes from officer field reports where relevant.

**Typical Jammers**

Most GPS jammers are quite simple devices offering a single jamming frequency which blocks the GPS L1 band used by satnavs and phones. These are generally quite low power and powered by inserting into the cigarette lighter or vehicle auxiliary power socket. We have recently seen USB powered devices. There are also battery operated devices and more sophisticated, more powerful multi-channel devices covering not only GPS, but mobile phone frequencies, Bluetooth which can be used in CCTV backhaul, Lojack and car key fob frequencies.


These jammers are mostly available from Chinese web sites and the sites generally lie about the range by considerably understating the operational range. However one has to discriminate between operational or damage range and detection range with the latter being much greater. Tests with detector technology have shown that a 3 watt jammer is detectable up to 6km away. Even the lowest power devices are detectable up to about 50m away. This is really good news for law enforcement applications as it means that officers can detect the jammer from a considerable distance away such as the opposite carriageway on a motorway.

New jammer types are turning up all the time and are less obtrusive and more likely to be overlooked in a police search. Jammers are not just the traditional cigarette lighter variety, they can also plug into the USB socket and OBD box.



**GPS Jamming Detector Technology**

There are currently three types of GPS jamming detector technology available from Chronos. Two are hand-held detectors and are currently in manufacture. The third is a GPS jammer photo trap device known as JammerCam which is currently undergoing field trials. All three types have been extensively tested at GPS jamming trials at Sennybridge which are managed and administered by the Defence Science and Technology Laboratory (Dstl) on behalf of the DE&S GPS Project Office and are authorised by MoD Joint Spectrum Authority (JSA).

The basic device, the CTL3510 is a small hand-held unit which can either fit in a pocket or attach to the vehicle windscreen in a suitable holder. When it senses GPS jamming, LEDs light up and the unit vibrates. It also logs the date and time of the event for future post processing.

The model CTL3520 is slightly larger and has the ability to direction find (DF) the source of the jamming signal. It's more sensitive than the CTL3510 and is best operated in a two handed mode. Its DF capability is sensitive enough to pick out a person carrying a jammer in a crowd or a vehicle parked in a busy car park.

The CTL3530 is the GPS jammer photo trap unit known as JammerCam. JammerCam is designed to be pole mounted and to scavenge power from a nearby lamp post. This will photograph a vehicle carrying the jammer and email the photo to a PC or smart phone. On-line access to the web site enables event and vehicle photo viewing and event statistical analysis such as number of events per month, per day, by day of week and by hour of day. There is a user editable notepad against each event. This enables officers to keep an on-going record of follow-up activity.

**Use Cases**

1 **General Jammer Use – Ofcom**

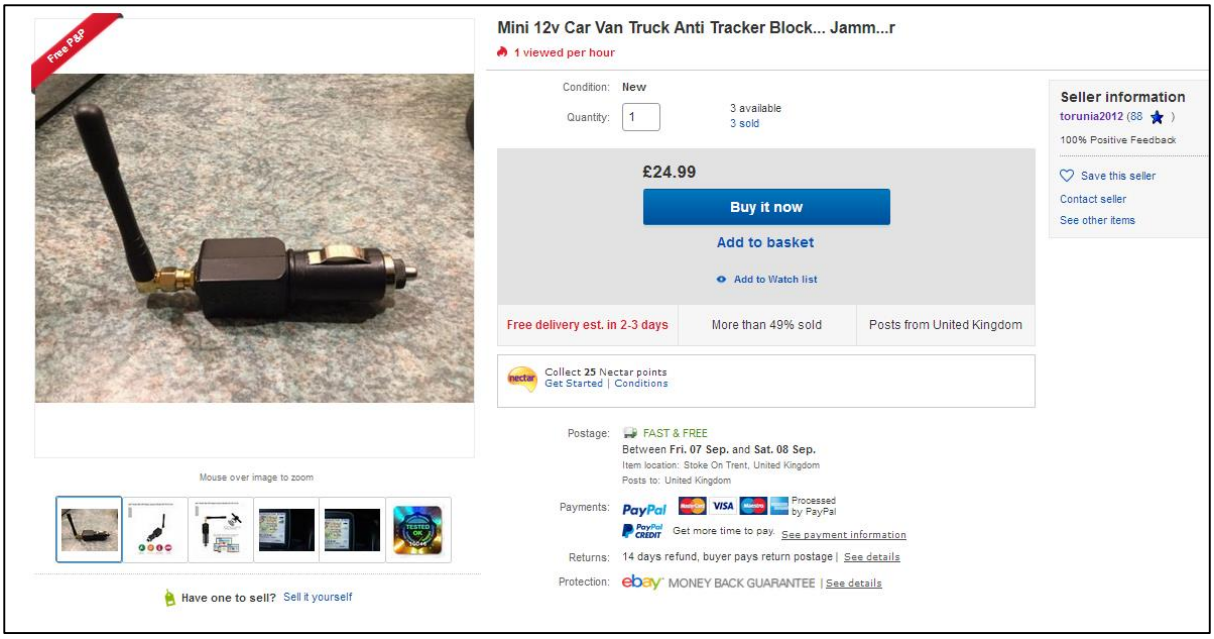
According to Ofcom general jammer use is an offence under the Wireless Telegraphy Act 2006 Section 68 with a maximum of 2 years in prison and unlimited fine**.**

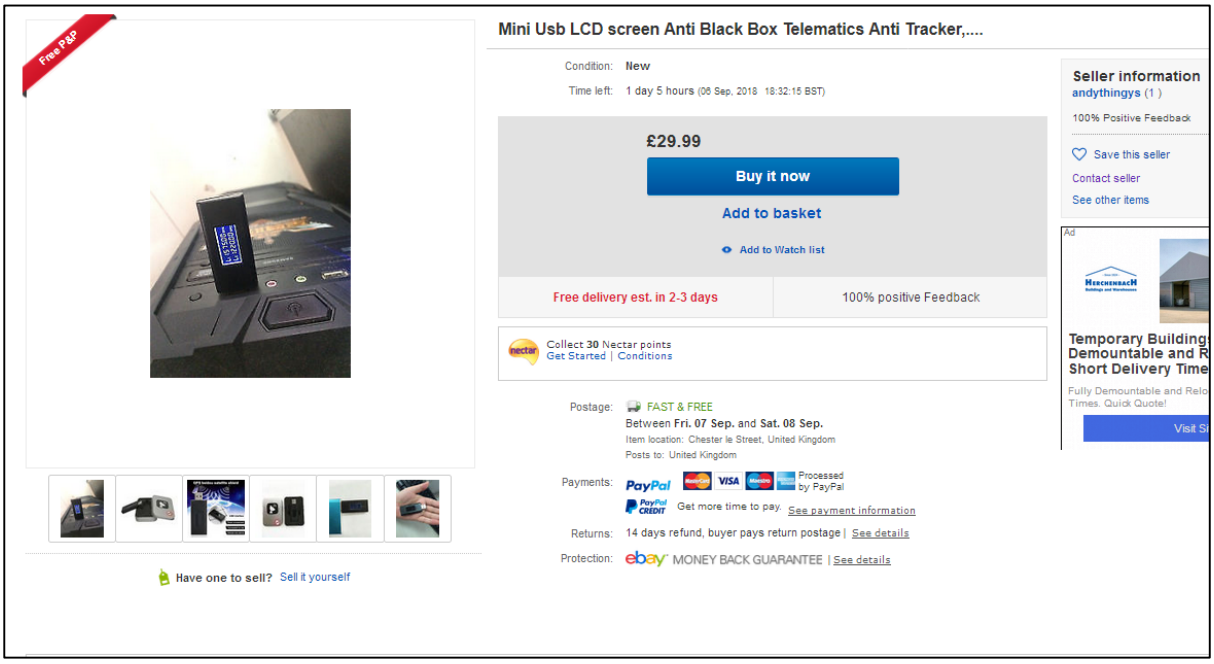
It is also an offence to supply jammers under the Electromagnetic Compatibility (EMC) Directive 2014/30/EU, which has been implemented into UK law by the Electromagnetic Compatibility Regulations 2016 (S.I. 2016/1091),

https://www.ofcom.org.uk/spectrum/interference-enforcement/spectrum-offences/jammers

Despite this you can buy jammers off eBay from UK sellers. This would suggest that nobody is doing anything to stop the sale or prosecute sellers. A few years ago when Ofcom "discovered" jammers, they contacted eBay sellers and confiscated stock.

See below a couple of current screen grabs of different sellers on eBay.




What of these eBay sellers. Are they not inciting people to break the law?

This is the marketing spiel o the web site. Corrected for poor spelling!

“Mini USB LCD screen Anti Black Box Anti Telematics Anti Tracker Ideal for company car/van drivers, young drivers and cheating spouses. It simply works by plugging into a USB socket in your car and can also be powered using a mobile phone power bank and no software is needed.

If your vehicle is fitted with a tracking device or a black box installed by an insurance company this will stop the insurance company and your employer from knowing where you are. Young drivers have black boxes fitted to keep the insurance premium down and if they go over the mileage allowance set by the insurance company they have to pay more.

Why pay more? Plug in before switching on ignition and as far as anyone knows, your vehicle is still at its last known location.

UK Seller. Fast free Royal Mail Signed For Postage."

**2 GPS Tagged Offender Tracking**

GPS tagged offender tracking technology is being piloted in the UK. There appears to be no evidence of any testing with GPS Jamming technology to assess the vulnerability or susceptibility of the tracking technology to loss of the GPS signal.

It is likely that the tag will cease to report its position when GPS is jammed. This should be tested as part of the pilot scheme.

It's also interesting to note that the MoJ publication available over the Internet "Electronic Monitoring GPS Satellite Tagging" handbook informs wearers that "The tag sends signals to a satellite 24 hours a day". This suggests that the team behind the GPS tagging programme has no idea how GPS works. GPS is a receive-only signal not capable of re-broadcasting a message from a GPS tag!

The tag will know where it is if there is a clear line-of-sight view to the sky. GPS tags will not work indoors, in tunnels or basements, blocks of flats, in well insulated environments e.g. new build with "Kingspan" insulation, under thick tree cover, garages, urban canyons, Underground trains, in ship's cabins or indeed anywhere where clear-sky view is disrupted.

The tag on an offender traveling away from the home beacon, but inside the curfew period is programmed to vibrate with red LEDs if the offender enters an exclusion zone or leaves an inclusion zone. A hypothetical use-case scenario may be using a pocket based battery operated multi-channel GPS/GSM Jammer. That would ensure that the offender disappears from view by the monitoring centre until the jammer is switched off. The monitoring centre would be none the wiser.

Pocket sized low cost GPS spoofers are now being demonstrated which can broadcast false GPS position signals. Instead of using a jammer which would kill the GPS signal, a low cost spoofer would continue to broadcast false GPS signals which the tag would pick up indicating that (for example) the offender was in their inclusion zone, whereas they could now be travelling into their exclusion zone. The monitoring centre would think they were behaving themselves.

**3 Young Driver Using Telematics or "Black Box" Insurance.**

Driver would use a jammer to defeat the ability of the telematics system to communicate location. The back office recording system would register the vehicle as being located at the location where the jammer was switched on, e.g home, garage etc.

What is the position regarding the validity of the insurance? Is the driver now driving without valid insurance? This is an example of there being a case to educate the insurance industry and get a view from the Ministry of Justice. Indeed if the MoJ were to pronounce on

the insurance validity issue, it might encourage wider usage of GPS jammer detection technology. See also Use Cases 3 and 4.

http://www.keepingyourlicence.co.uk/insurance

Recently in July 2018, Hampshire police seized a jammer from an 18 year-old who was using it to evade his young driver curfew times. The insurance company had not heard of this evasion tactic and have subsequently cancelled the policy. Apart from the aspect of invalidating the insurance policy, the driver's actions were considered to be "Insurance Fraud".

Penalty: Driving without valid insurance is a criminal offence and could receive up to 8 penalty points, a maximum fine of £5,000 and a possible driving ban.

**4 Van and Truck Drivers Using a vehicle equipped with Fleet Tracking Technology**

Driver would use a jammer to defeat the ability of the fleet tracking system to know where the vehicle is. The back office tracking system would register the vehicle as being located at the location where the jammer was switched on, e.g home, garage etc.

Driver would use a jammer to defeat the GPS technology that is embedded in and enables smart tachograph technology which will be mandated on UK roads under the Traffic Act in 2019.

Driver would use a jammer to defeat "Driving Hours" regulations as managed by smart tachographs.

**Taking Without Consent (TWOC).** TWOC is a summary only offence and can only be dealt with in the Magistrates Court where the maximum sentence that can be imposed is 6 months imprisonment and/or an unlimited fine.

https://www.sentencingcouncil.org.uk/offences/item/vehicle-taking-without-consent-revised-2017/

The driver is also driving without insurance (see Use Case 2 and 4) and committing an offence under the Wireless Telegraphy Act (see above Use Case 1).

Case Study #1

Sat 6th Jan 2018: Gloucester Services - Hewar Van - Fleet Tracking Avoidance. "A marked traffic car was travelling on the M5 from junction 12 to 11a when the jammer detector, CTL3510 was activated in their traffic car. The officers turned at junction 11a and travelled south, they caught up the van, with the device still activating & then got in front of the van & put up their matrix board 'follow me' and the van followed them into the service area at Gloucester Services (hence the JammerCam activation). As the officers walked up to the van they could see the jammer

plugged in to the cigarette 12v socket. Officers approached the male & seized it. He stated that he was using it so that he could leave work early, so that his bosses did not know that he was leaving work early. The device is with Gloucestershire police now. The van driver had no idea how the device had been detected. He was aware that it was an offence. See Case Study and video.

Case Study #2

Weds 17th Jan 2018: In this example the jammer detection led to petty crime detection. Chandlers Ford Asda – CTL 3510 detection (Hampshire Police) - Shoplifter, failed breathalyser test, fleet tracking avoidance. See Case Study.

Case Study #3

Detections by PC 2531 Paul Townend of Hampshire Police in April 2018

*"The same day and was a moving works van which I passed in the opposite direction. I turned around on my bike and stopped the van. The jammer was in view and he stated that he had been working and was allowed to take the van home but had decided to go and have a look at the car boot sale nearby and so had put the jammer in. Another telecoms detection and verbal warned re the technical TWC."*

Case Study #4

*"A moving vehicle (UK registered artic) which we passed on a dual carriageway. Stopped near Ealing wharf at Totton with the jammer plugged into the cab. Driver was Lithuanian and even with an interpreter communication was difficult. He stated that he had plugged it in an hour ago and was delivering some empty pallets to the wharf. The back was checked and there were some empty pallets but no cars or plant. I spoke to his boss (transport manager) on the phone who confirmed that they do exchange pallets so I could not prove any TWC which left me wondering WHY he was using it? I never did get this out of him but I couldn't prove any major crime. Another detection for the telecoms offence."*

Case Study #5

Follow up to last month's Portsmouth JammerCam event with a DAF truck - PN67 UPD 14/9/18.

From PS 1463 Paul Diamond, Hampshire Constabulary Commercial Vehicle Unit and Force Hazmat Advisor.

*"This was added to my CV ANPR hotlist and intercepted a few days ago on the A34 for a check.*

*Whilst the jammer was not active at that time we downloaded the tachograph and used the Inelo Tachoscan software to analyse the driver's hours data.*

*There were incidents of driving with two cards, daily rest and daily drive offences. Infringements directly related to road safety, fatigued driving and setting a fair playing field for haulage enterprises.*

*Possibility that driver was using jammer in an attempt to hide the telematics that would potentially give away the route or timings for unlawful activity. Might be that he didn't fully understand how his particular unit worked. Could also be for another reason.*

*Roadside GFPNs issued to the value of £600 and the driver will be going to a traffic commissioners enquiry with regard to his behaviour. As an owner operator there is a chance he may lose his licence to operate.*

*A good example of using one piece of intelligence data to target a stop and then more thoroughly examine for other, potentially linked digital evidence of offences."*

5 Truck Drivers evading road toll charging technology.

Driver would use a jammer to defeat the GPS technology that is embedded in and enables smart road toll charging.

Belgium brought in the Viapass Kilometre Charge toll in 2016. Vehicles are fitted with a GPS enabled "On Board Unit" (OBU)

https://www.viapass.be/en/news/single/article/the-kilometer-charge-for-heavy-goods-vehicles-of-over-35-tonnes-enters-into-force-on-1st-april-201/

6 Enabling the theft of high value cars and plant by evading Tracking Technology.

Many high value cars and plant are "protected" by commercial tracking systems such as "Tracker" which enable a back office system to locate the stolen vehicle after the theft is reported. Some systems use technology other than GPS to locate the vehicle. This could be a VHF (Lojack) frequency to transmit location or cell ID to transmit approximate location.

Multiple frequency jammers are now available which jam not only GPS but also the mobile phone frequencies and the Lojack frequencies. Some will also jam the key fob keyless car lock systems, effectively disabling the ability to remotely lock the vehicle and enabling a quick getaway by using key cloning technology plugged into the OBD unit.

This news item covered a spate of thefts from cars on the M4 in 2016. https://news.sky.com/story/hi-tech-car-theft-warning-to-drivers-at-m4-service-stations-10680370

7 Evading covert vehicle tracker technology

Evidence of this activity has come from discussions with people who have been expert witnesses at OCG crown court sessions. One particular case in 2017 "Operation Escalade"

received significant publicity and used a briefcase style multi-frequency jammer referred to as “counter surveillance” equipment. Scroll down to see a picture in this article.

http://www.dailymail.co.uk/news/article-5168725/Brutal-sophisticated-Scottish-gang-snared.html

8 Hi-jacking valuable loads

We have heard about a South African hi-jacking where the hi-jackers followed the target vehicle with a powerful jammer. This caused the target vehicle’s tracking technology to fail giving the impression back at the fleet tracking centre that the truck had stopped. A few miles further on the hi-jackers pulled the vehicle over and removed the load safe in the knowledge that if alerted, the police would not be looking in the right place.

The following two case studies are from Mexico where our local channel has been working closely with the Federal Police.

**Pacifico Beer Hijack**


“We were undertaking a joint crime prevention operation in mid-August with Mexican Police using the Chronos GPS Jamming detectors CTL 3510 and CTL 3520. Whilst the operation was underway the officer-on-duty received a call from a fleet tracking company, reporting the theft of a truck owned by Aldafa Transportes https://www.aldafa.com.mx/. They had lost contact with the truck which was being tracked on the Durango highway near Torreón.

The last known location was communicated to the officer-on-duty at the Mexican Federal Highway Police as part of the search and location contract in operation. As the officers were relatively nearby they were able to head towards this last known location and using the detectors managed to pick up a jamming signal about 120m away, before the truck was actually in sight. As they got closer the jamming signal got more powerful and then finally they were able to make a positive ID as they drew alongside.

The truck was transporting pallets of Pacifico beer, with a value of approximately $1,000,000 pesos (about £40,000). The driver, a Mexican, 46 years of age was arrested along with his passenger who was also Mexican and 25 years of age. It transpires that the younger man is an employee of Aldafa and he admitted that he was the original driver and – it seems likely – a co-conspirator to the hijack. The

white pickup was the look-out vehicle. A common feature of Mexican hijacks. A black six-antenna unbranded (3W) GPS Jammer was discovered in the cab."

**New Kenworth Trucks Hijack**

Mexican Federal Highway Police were undertaking a crime-prevention operation on 26th August with the Chronos CTL 3510 and CTL 3520 GPS jamming detectors. They were informed by the officer-on-duty that he had received a phone call from the Kenworth company https://www.kenworth.com/, reporting the theft of three of their new semi/artic tractor units which had been travelling in convoy on the toll-free highway to Yahualica de González Gallo in Jalisco state. This was the last known location that had been registered on the tracking system before they disappeared. Their disappearance over approximately 10km of the highway triggered the contracted operational search and location procedure.

Three brand new model 2018 Kenworth trucks, which were being delivered to a dealer had disappeared – colour's red, white and blue, but with no other company branding or registration plates. They were worth approximately $3,000,000 pesos (£120,000) each.

The Chronos GPS jamming detectors picked up the jamming signal well before the trucks were in sight and then the officers were able to identify the trucks as they got closer. There was a shoot-out as they attempted to pull the trucks over and then the three trucks went off-road to try and lose the officers. The trucks were found as each had an unbranded (3W) GPS jammer with no serial number and with six antennas. Their whereabouts was identified using the Chronos CTL 3510 and CTL 3520. Two of the drivers ran off and got away but another two were arrested at the scene.

**False Positives**

Sometimes the interference detection technology will detect radio frequency interference (RFI) that is not a true jammer. This is referred to as a false positive event. Typical false positives include:

- Badly installed GPS antennas. The weak GPS signal from the sky is amplified after the antenna. If it meets a bad connection on the way into the satnav unit or embedded GPS application it can bounce back out of the antenna and be sufficiently powerful to trigger the

detector technology. We have seen a number of cases of satnav installs in Mercedes saloons that have exhibited this behaviour.

Example of a "False Positive" detected by PC 2531 Paul Townend of Hampshire Police 10th April 2018

*"Yesterday I was on the bike coming up the A326 at Holbury and got a fairly good detection as I passed by the co-op where there were a couple of vans parked. I spun around and tracked the signal to be coming from an Iveco Daily Luton bodied delivery van which was parked up on their forecourt. The signal was approximately half strength as I passed by at a distance of around 40 Meters and went to full strength when by the cab or inside the cab.*

*The drivers work for a company who deliver mixed large goods such as beds and bathroom suites which is what they had loaded. They have a hand held scanner which they use to record deliveries. This device is GPS enabled and has its own battery which gets charged when in the docking port fitted in the cab. It transpired that it was this unit that was giving out the jamming signal but only when it was powered up AND had the GPS signal connected.*

*This took some finding and searching of the cab and vehicle. No jammer was found and the driver who was "no trace" on PNC appeared genuine and appeared to have no knowledge. Apparently there is no GPS tracking on the van itself but there is on the scanner device."*

**Unexplained Interference**

In the context of detecting criminal behaviour through detecting GPS Jamming, unexplained interference could be an indicator. By unexplained interference we mean that the CTL3510 indicates interference but the CTL3520 has trouble indicating the direction of the source due to local multipath.

The source will be a fixed location. It could be a radio Ham as probably discovered by Ordnance survey during an interference search after they were subjected to intermittent interference to one of their differential GPS reference stations. It could however indicate OCG activity such as a "chop shop" or drug dealing.

Chop shop activity has been known to use fixed, relatively high power battery operated, mains rechargeable jammers as a counter measure to vehicle tracking technology which may be fitted to newly arriving stolen cars. One such chop shop was found because they forgot to switch the charger on at the mains and the battery ran out!

Picture here shows a jammer recovered from a chop shop in Kent during July 2018

Drug dealing from a private house may be another source of jamming. In this case a multi-frequency jammer which not only jams GPS but also the GSM mobile phone bands may be used. This would be used to disable mobile phone tracking Aps.

A fixed jamming case in Montpelier, Cheltenham in November 2017 has not so far been resolved.

This kind of jamming should also be of interest to Ofcom especially as it may be powerful enough to adversely impact nearby critical infrastructure.

**Conclusion**

The GPS jammer detector trials work with Gloucestershire and Hampshire constabularies is beginning to inform the law enforcement community knowledge-base regarding GPS jammers and the reasons why people use them for different applications. Whereas originally it was thought that jammer use divided into criminal and non-criminal use. It would be more appropriate to divide it into deliberate criminal use i.e. OCGs and uses in drugs and car/plant theft, medium criminal use such as evasion of offender tracking technology and evasion of smart tachograph driver time monitoring to unintentional but nevertheless relatively serious criminal use e.g driving without insurance and taken without consent.

GPS jamming has been with us for ten years and is still relatively new to most Police Forces. GPS spoofing is an emerging threat with no known applications outside of hacker convention demonstrations e.g Defcon. This is a fast changing cyber-physical landscape with new threats and new use-case scenarios evolving all the time. We can't afford to be complacent.

Prof. Charles Curry BEng, CEng, FIET, FRIN

Chronos Technology Ltd

www.chronos.co.uk

Bio

Charles Curry is a Chartered Engineer, a Fellow of the Institution of Engineering and Technology (IET), and the Royal Institute of Navigation (RIN), and founder & Managing Director of Chronos Technology Ltd. Charles graduated in Electronics from Liverpool University in 1973 and started his career at GEC Hirst Research Centre working on silicon MOS boundary research, progressing to Racal Instruments where he was responsible for sales of test equipment including specialist frequency and time products such as Loran C and Caesium standards. Later with GSE Rentals, Charles was involved with some of the first civil GPS and laptop PC deployments into the North Sea offshore oil exploration industry during the early 1980s.

He founded Chronos in 1986, a leading global system integrator, service solutions provider and manufacturer for synchronisation, timing, GNSS and GPS jamming detection products based in the UK. Chronos has supplied and installed many thousands of GPS & Timing systems worldwide for mobile and fixed-line telecom operators. The Chronos Synchronisation MasterClass has been delivered to more than a 1000 delegates across the globe.

Charles founded the International Timing & Sync Forum (ITSF) in 2001 and chaired the ITSF Steering Group until 2017. He has also been a member of the USA Workshop on Synchronization in Telecommunications Systems (WSTS) Steering Group for many years. Charles is also a member of the Industry Advisory Boards for the Universities of Liverpool and Bath, Electrical and Electronics Faculties.

Charles has contributed to The Royal Academy of Engineering reports on “Global Navigation Space Systems: Reliance and Vulnerabilities” and “Extreme Space Weather: Impacts on Engineered Systems and Infrastructure”. Also the UK Government’s Blackett Report on “Satellite Derived Time and Position: A Study of Critical Dependencies”

In 2012 Charles was awarded Honorary Professorships from the University of Bath, Faculty of Engineering & Design, Department of Electronic & Electrical Engineering and the University of Liverpool, Department of Electrical Engineering & Electronics.

In 2018 Charles was awarded the Royal Institute of Navigation’s 2018 Duke of Edinburgh’s Navigation Award for Outstanding Technical Achievement in “Recognition of technical excellence and authority in satellite navigation and timing vulnerabilities and mitigations”.