SENTINEL PROJECT

REPORT ON GNSS VULNERABILITIES

SENTINEL Project – GNSS Vulnerabilities

The SENTINEL Project investigated a number of interconnected activities involving mission-critical or safety-critical services which need to be able to "trust" GNSS signals at the point of use. The SENTINEL Project was concerned with GNSS interference and jamming, and techniques for mitigating such jamming. This Report also records some of the world-wide press and television coverage stimulated by presentations of the results of SENTINEL at numerous conferences and symposia.

Registered in England No. 2056049. Registered Office: Stowfield House, Upper Stowfield, Lydbrook, GL17 9PD.

VAT No: G.B. 791 3120 44

N.B. Only documents bearing the Document Status 'APPROVED CHRONOS DOCUMENTATION' in the panel below are deemed official literature.

Originated by:	Prof. Charles Curry. BEng, CEng, FIET	Title: Managing Director, Chronos Technology
Document Status:	**RELEASED**	SENTINEL Project – Report on GNSS Vulnerabilities

07 February 2014

RECORD OF ISSUE

Issue	Date	Author	Reason for Change
001	11/02/2014	CC	Final for Release

TABLE OF CONTENTS

LIST OF FIGURES

LIST OF TABLES

1 EXECUTIVE SUMMARY

The SENTINEL project has been supported by the United Kingdom Technology Strategy Board (TSB). Its roots lie in an earlier TSB-supported project, GAARDIAN. SENTINEL set out to examine various aspects of the emerging threat from low-cost commercially-available GPS jammers. Whilst those who have been close to the project now take the threat from such jammers almost for granted, this was not the case when the work began in 2008. Matters that now seem clear were then emerging unknowns still requiring corroboration, expert knowledge, testing and trials.

This report brings together diverse aspects of SENTINEL. These include: the SENTINEL platform; long-term test results from it; descriptions of jammers and identification of their provenance; descriptions of trials using jammers; videos and press articles arising from SENTINEL exploitation and dissemination activities; and a review of areas in which research would be justifiable in future.

The project has found that the problem is clearly getting worse with some locations detecting 5 to 10 events per day; over 50 web sites selling jammers and law enforcement seizing much more powerful jammers with much greater ranges and coverage. Whereas GPS was the only satellite PNT system under threat in 2008, now it is all the GNSS frequencies including Galileo.

One important conclusion has become evident from the work on GAARDIAN and SENTINEL over the past 6 years: the GPS jamming threat is getting worse; most people don't yet 'get it'; and a 'Black Swan'[1] event will happen in the UK, just as has already occurred in South Korea.

For further information relating to this Report – please email SENTINEL@chronos.co.uk

2 GENERAL

2.1 SCOPE & APPLICABILITY

According to the recent Royal Academy of Engineering report on the Vulnerabilities of Global Navigation Satellite Systems (GNSS)[2], GPS jamming presents a clear threat. But that threat is still barely recognised by many of the organisations responsible for operating mission-critical or safety-critical services in the UK. Whether these organisations are in denial regarding the threat, or are simply oblivious to it as they struggle to manage more pressing issues, is a matter for conjecture – and certainly a subject for education! Nevertheless, the conditions are present for a catastrophic 'Black Swan' event.

Seeking to address these matters, the SENTINEL (GNSS SErvices Needing Trust In Navigation, Electronics, Location & timing) project has built on strong foundations. These were laid down in the earlier TSB-supported project GAARDIAN (GNSS Availability Accuracy Reliability anD Integrity Assessment for timing and Navigation). SENTINEL has investigated a number of interconnected activities involving mission-critical or safety-critical services which need to be able to "trust" GNSS signals at the point of use. The Report describes two specific areas covered during SENTINEL: GNSS interference and jamming; and techniques for mitigating such jamming. It also records some of the press and television reports world-wide, stimulated by presentations of the results at conferences and symposia. This Report focuses on interference and jamming to GNSS and the role of Enhanced Loran (eLoran) as an important mitigation technique for GNSS vulnerability.

2.2 ACRONYMS AND ABBREVIATIONS

See APPENDIX E

[1] Black Swan Event: http://en.wikipedia.org/wiki/Black_swan_theory Nassim Nicholas Taleb
[2] Royal Academy of Engineering – Report on GNSS Reliance & Vulnerabilities

3 INTRODUCTION

This report presents results from the SENTINEL research project supported by the UK Technology Strategy Board (TSB) under the "Trusted Services" Call. SENTINEL examined the growing threat of GPS jamming. In practice, this would appear to be caused principally by low-cost commercially-available jammers. The Report assesses the impact of such jamming.

GAARDIAN, the project that preceded SENTINEL, was also supported by TSB. It was part of the "Gathering Data in Complex Environments" programme. Its role was to create a data-gathering system that could be deployed close to the sites of mission-critical or safety-critical activities. There it would certify the accuracy and reliability of Positioning, Navigation and Timing (PNT) sources, specifically the signals of Global Navigation Satellite Systems (GNSS) and especially GPS. The technical challenge for GAARDIAN was to gather and filter continuously large volumes of data from dispersed locations whilst retaining their contents. The research project stimulated the opening-up of new markets, especially those concerned with safety-critical navigation and timing application, including homeland security. GAARDIAN moved the UK into a leading position in the commercial exploitation of future systems for monitoring the integrity of mission-critical PNT sources.

When SENTINEL evolved from GAARDIAN, its role was to establish the degree of reliance users could place on GNSS and eLoran Positioning, Navigation & Timing (PNT) signals. A network of SENTINEL probes would be deployed to monitor key parameters on a 24x7 basis. They would detect, quantify and locate natural and deliberate GNSS interference. Examples of natural interference are space weather events and multipath propagation in places where satellite signals are blocked and reflected. Examples of deliberate events include GPS jamming by criminals and others. SENTINEL results would enable decisions to be made on the degree to which a PNT service for safety-critical or mission-critical applications could be trusted and what impact interference would have on their security and their ability to generate revenues. SENTINEL probes would also provide alerts that would enable users to identify and quantify jamming events and help agencies with a remit to protect critical national infrastructure, such as roads, ports, railways, harbours and airports, mitigate them.

4 BACKGROUND AND SCOPE OF THE RESEARCH

4.1 THE SENTINEL PROJECT

The main component of the SENTINEL is a national network of GPS interference and jamming sensors. These are hosted at locations of opportunity provided by SENTINEL collaborators who include the Ordnance Survey (OS), the National Physical Laboratory (NPL), the Association of Chief Police Officers (ACPO-ITS), National Air Traffic Services (NATS), the General Lighthouse Authorities of the United Kingdom and Ireland (GLAs), and the University of Bath (UoB). All these sensors include GPS receivers and many of them also have eLoran receivers. They operate remotely and continuously.

The sensors identify anomalous GPS events by deploying algorithms developed as part of the SENTINEL programme. The algorithms, which have been designed to eliminate false-positive data, were devised by the University of Bath and Chronos Technology. In addition, a Quality of Service (QoS) algorithm was developed by GLAs as part of their programme to explore the effectiveness of the eLoran low-frequency Positioning, Navigation and Timing (PNT) signals as a complement to GNSS, capable of mitigating its vulnerability.

When a GPS jamming event is detected it is reported to a central server hosted at Chronos Technology. The communications employ VPN links over LAN connections supplied by the organisations that host the sensors or via 3G data links; 4G links are now being trialled. This system has not only continued in use, but actually developed further, since the ending of TSB support. GAARDIAN and SENTINEL employed early examples of "Machine to Machine" (M2M) communications, "Cloud" computing and "Sensors over the Internet", techniques whose use has now become much more widespread.

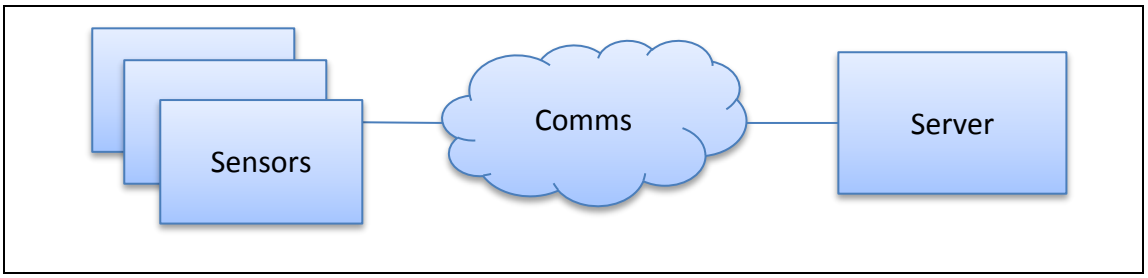

Figure 1: Architecture of the SENTINEL System

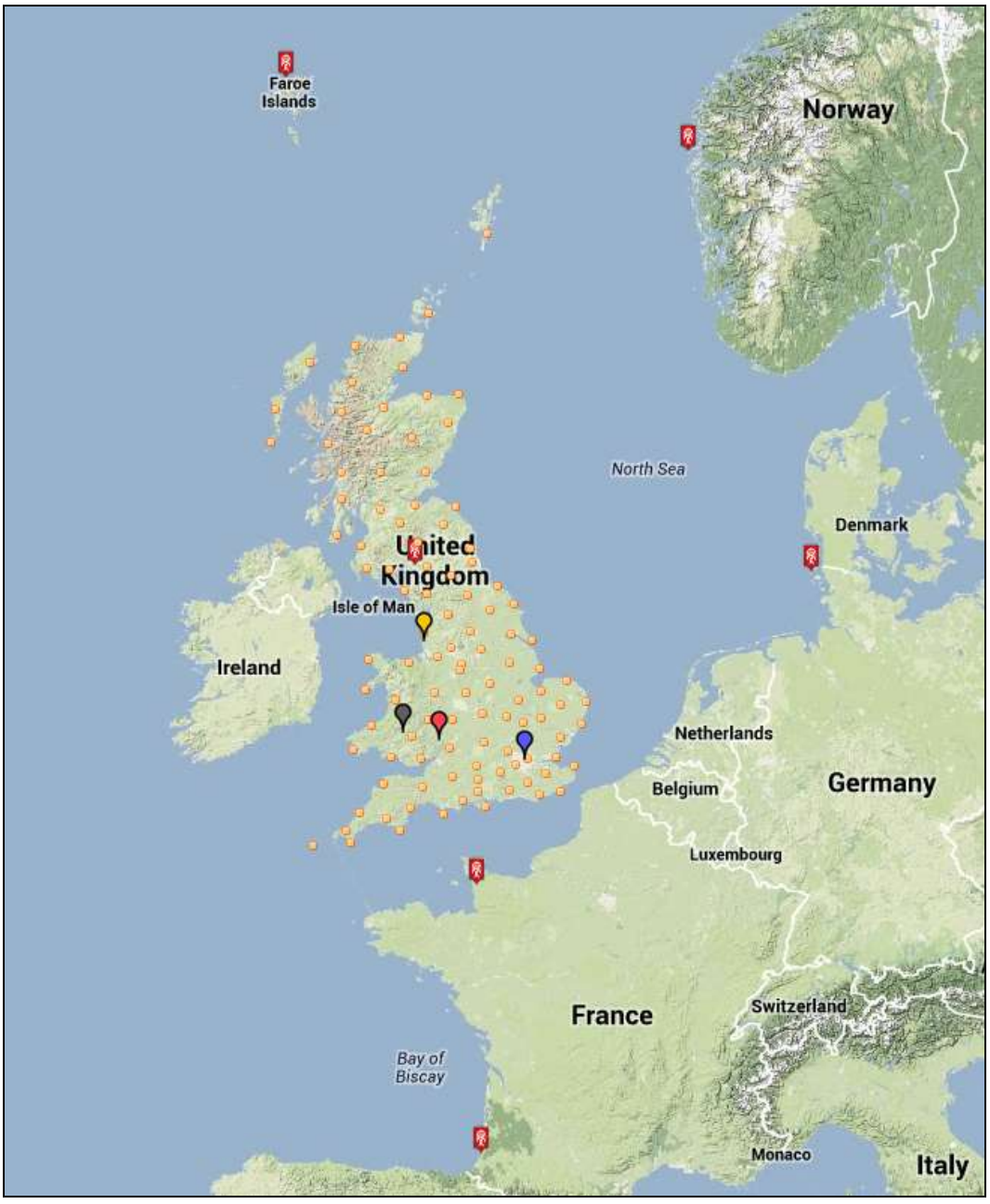

Figure 2: SENTINEL Map GUI

The locations of some SENTINEL sensors are shown in Figure 2, which is a screen shot of the SENTINEL Graphical User Interface (GUI). The significance of the colours of the markers is as follows: Blue – Operational sensors with no alarms; Yellow and Red – Operational sensors in various alarm states; and

Black – Dormant sensors or sites with historical data only. The eLoran transmitting stations such as Anthorn in Cumbria are marked by red flags. The yellow dots represent OS Net reference stations.

The GUI enables sensor settings to be adjusted to take into account the local GNSS reception environment. By this means it is possible to allow for the level of multipath propagation there, so minimising the occurrence of false positives. A user can also review and analyse data indicating jamming events detected by the sensors.

Map views can be customised to allow the various participating organisations to examine data from stations of their own network only; this helps preserve security. The GUI can also take into account the skill level and privileges of groups of users; some users are allowed to alter settings, while other only have the right to view the data.

Intelligence built into the SENTINEL sensors establishes when a GPS jamming event has been detected. The sensor then sends to the server an event time stamp and a 'photo' of the signature of the event, including a measure (adjustable by the user) of the level of background signal before and after the event. In this way the amount of data to be conveyed is substantially reduced: the development of this capability was a key deliverable of the GAARDIAN project. As a result, a 3G data link can easily accommodate a SENTINEL probe.

4.2 JAMMING EVENT DETECTION ALGORITHMS

Two quite separate techniques, both designed to identify jamming events, were developed within the SENTINEL programme. The first of these is a "multipath algorithm" called "QuickThresh" written at the University of Bath.

QuickThresh works by establishing the signal-to-noise (SNR) for each satellite in view, as determined by the GPS receiver in the sensor. It uses this to set an SNR mask (shown as the pink band in Figure 3) and continuously compares the measured SNRs (red line) with the mask values. During the jamming event shown, the pink band shows the SNR mask, in this case PRN 1. When the SNR, (shown by the red line) drops below the yellow trigger for longer than a user defined period (say 5 seconds), a jamming event is deemed to have occurred. A data record showing SNR values ahead of, during and following the jamming event is then captured. The blue line is the satellite elevation.

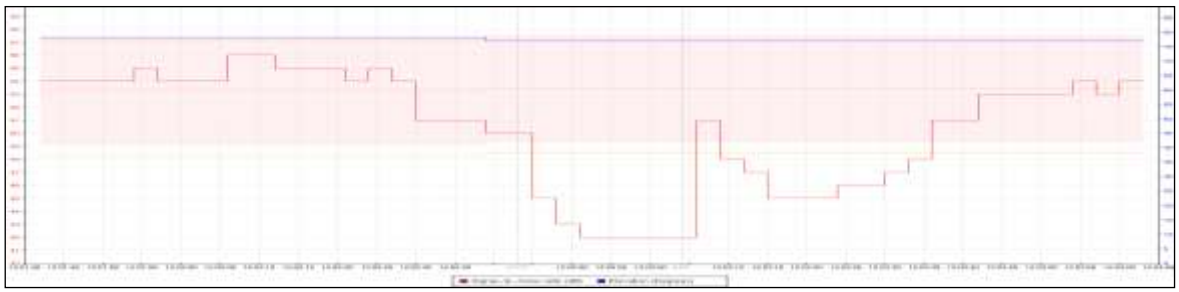

Figure 3: Jamming event caught by the UoB QuickThresh Algorithm

A second method of identifying jamming events was developed by Chronos Technology (see Figure 4). It employs a Fast Fourier Transform (FFT) technique. The FFT employs samples of the IQ data from a receiver tuned to the GPS L1 frequency. A local threshold, shown by the red line in the figure is established, based on the power of the background noise. If the received signal power at the GPS L1 frequency (shown here by the blue line) then exceeds the threshold for a user defined period (say 5 seconds), a jamming event is deemed to have occurred. When a jamming event has been detected, data is captured showing the relative power in the L1 spectrum before, during and after the event. The blue line represents the average relative power at L1.

The shape of the curve in Figure 4 is consistent with the following scenario: a vehicle approached the vicinity of the sensor, then passed behind a building (causing the dip between the two peaks), before moving away behind other buildings and eventually out of range of the sensor.

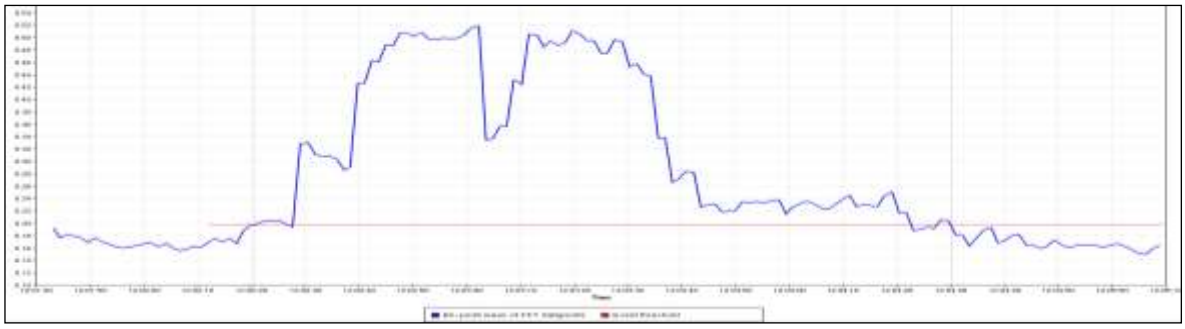

Figure 4: Same jamming event as Figure 3 caught by the FFT Algorithm

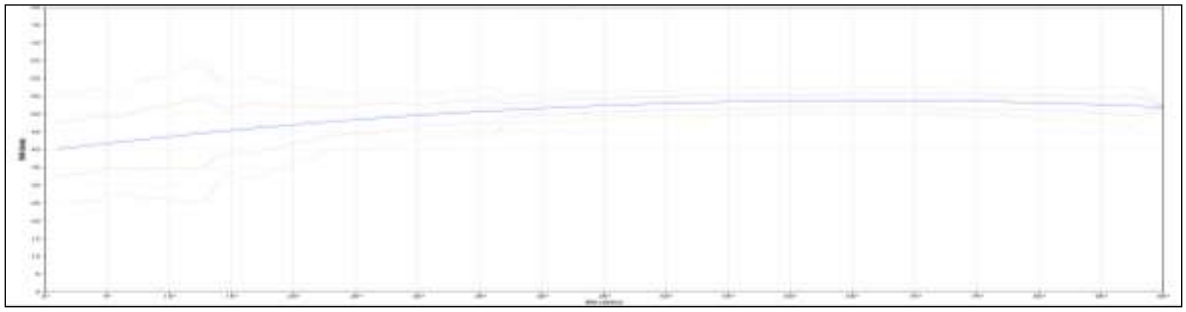

Figure 5: QuickThresh Mask

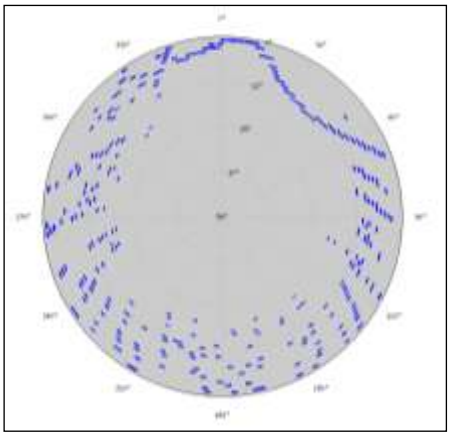

Figure 6: Multipath by Azimuth

A SENTINEL sensor can also be used to explore the degree of multipath propagation around its location. The system has been designed to allow the user to adjust all settings remotely, thereby maximising its value as a research tool. Its principal application is as a detector of locations at which there is a high level of multipath signals; such places are far from optimal for GPS reception. In Figure 5 the blue line represents the average SNR (Y-Axis) for all satellites with the X-Axis showing elevations from 0 to 90 degrees. The two red lines represent the +/-1 and+/-2 Standard deviations for location.

The GPS receiver in the probe outputs standard NMEA data streams which are sent via the data link to the server where they can be recorded.

4.3 FLEXIBLE FIELD DEPLOYMENT

Early in the project a decision was made that SENTINEL sensors should operate and communicate data continuously via the selected LAN/3G data link. The alternative arrangement, in which sensors equipped with on-board memory stores would be deployed temporarily, was deemed too cumbersome. Also, the time required to deploy and retrieve them would be excessive.

SENTINEL sensors have been deployed on behalf of many clients. This has allowed them to evaluate the nature and extent of any jamming problems in the vicinity of their critical infrastructure. Each client has a unique log-in. Alternatively, the server can be set to send the client an email when a jamming event is detected.

During 2013 SENTINEL has developed substantially. What was designed as a research platform for investigating the vulnerability of GPS has turned into a GPS Vulnerability Evaluation and Demonstrator platform. As such it is suitable for organisations which are considering deploying systems permanently; this concept will be described further in Section 8.2.

4.4 GPS (L1) JAMMING EVENTS AND SOME TEST RESULTS

While individual GPS jamming events can be examined in detail, long-term monitoring is also essential in assessing the threat at a specific location. The following graphs show SENTINEL data collected over many months at various sites around the UK. This monitoring operation has continued beyond the ending of TSB funding on 31 March 2013.

The data has been filtered to show events of more than 5 seconds duration only.

4.4.1 TEST RESULTS – MOTORWAY NEAR AIRPORT RUNWAY

These results show events that were detected on a motorway that passes only 200ft from the cabin that houses equipment for an Instrument Landing System (ILS) at a provincial airport.

The SENTINEL sensor is housed in the weatherproof enclosure on the right connected to the GPS antenna just above the ILS cabin.

Figure 7: SENTINEL Sensor beside ILS cabin

In the events analysis graphs shown below the Y-Axis represents the accumulated total number of events for the time period shown in the X-Axis

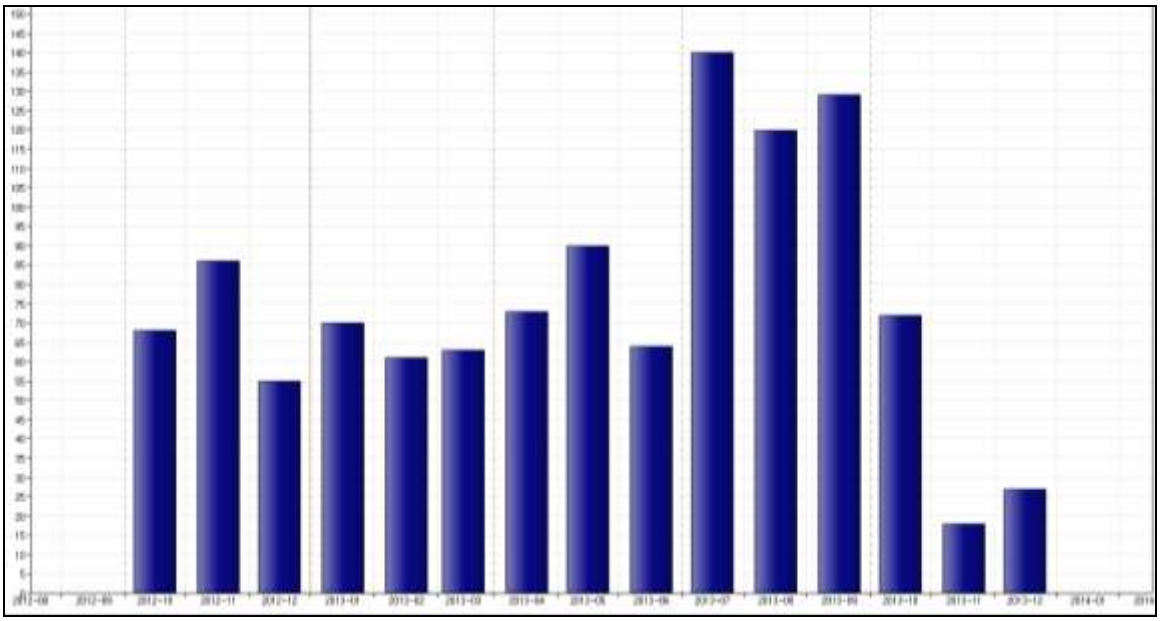

Figure 7: Totals of GPS jamming events detected in each month from October 2012 to December 2013.

The number of events shown during November and December 2013 may be less than actually occurred since some data was lost due to communications issues at this airside site of restricted access.

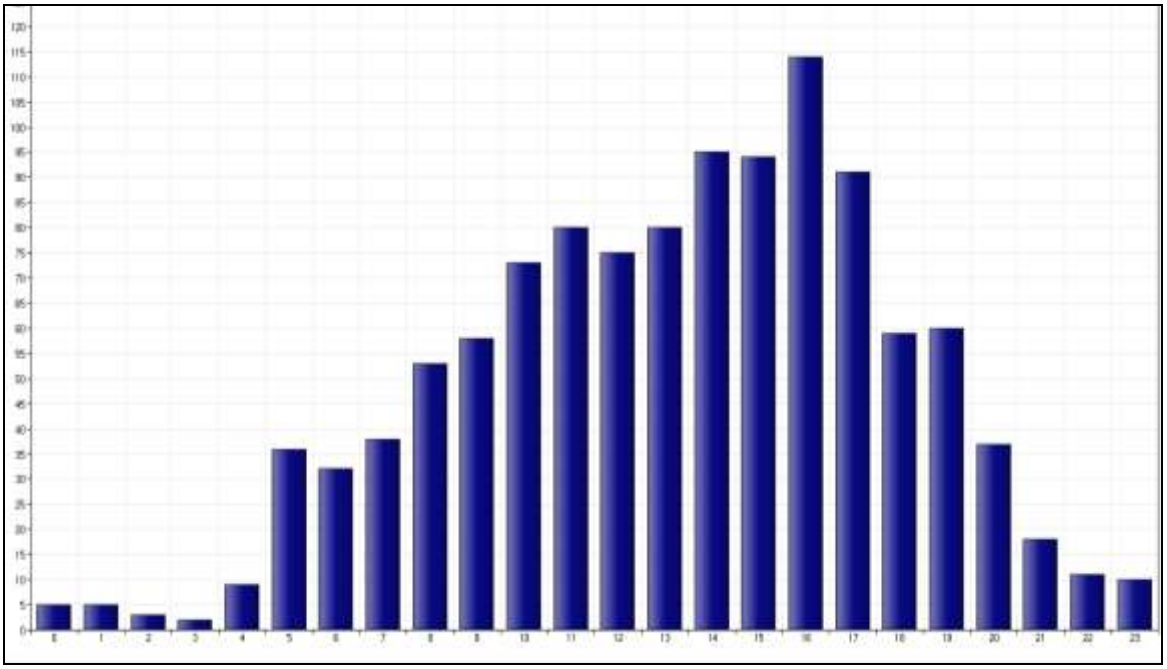

Figure 8: Totals of GPS jamming events detected in each hour of a day from October 2012 to December 2013

The X-Axis starts at midnight on the left. Each hour is the cumulative total of all events during the period covered in Figure 7. Note the very few night-time events at this site.

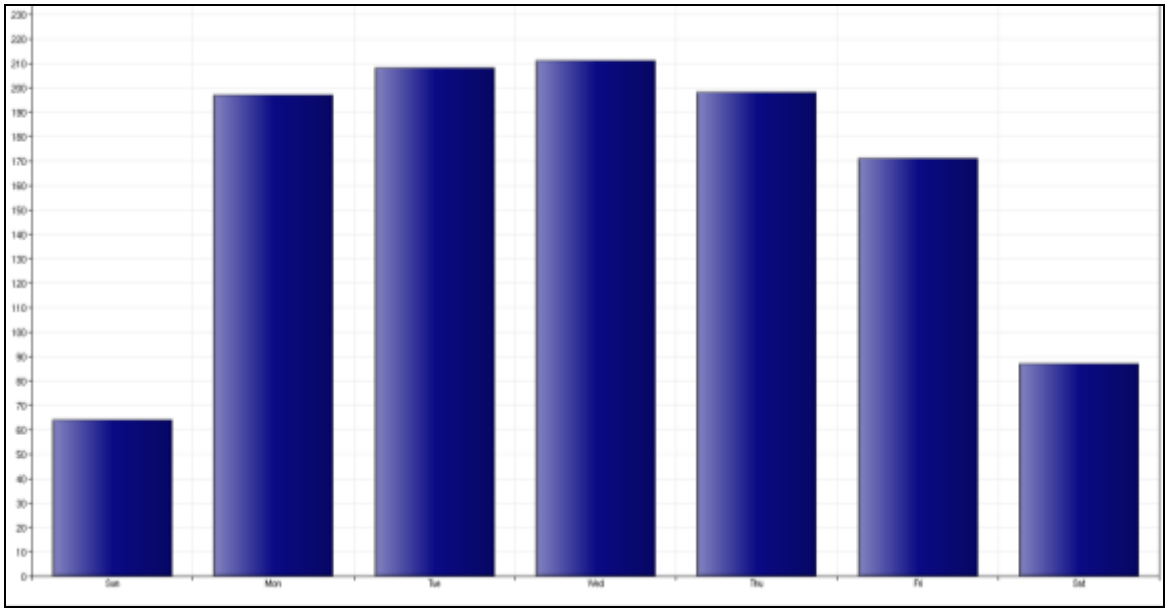

Figure 9: Totals of GPS jamming events on each day of the week from October 2012 to December 2013

In this graph the X-Axis represents the cumulative total of events by day of week starting with Sunday on the left for all events during the period covered in Figure 7.

Figure 10: Time signature of a typical GPS jamming event at this site.

The strength of the received interfering signal is plotted over a period of approximately 160 seconds. The duration of the broad peak is approximately 40 seconds.

4.4.2 TEST RESULTS – CITY OF LONDON

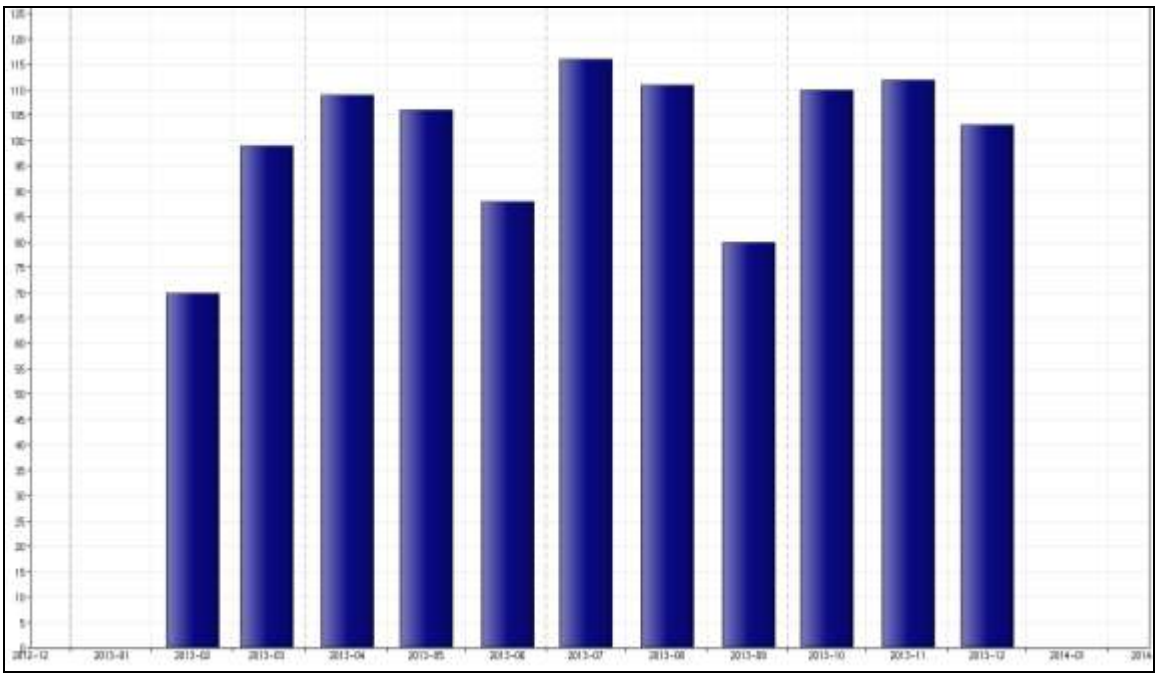

Figure 11: Totals of GPS jamming events in each month from February 2013 to December 2013

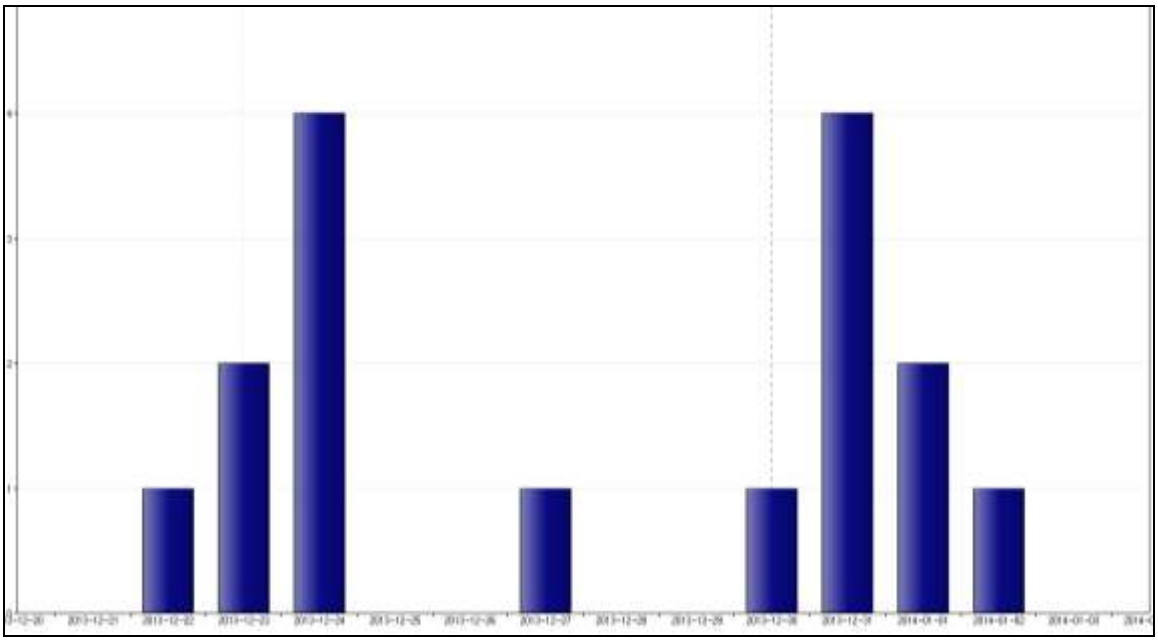

Figure 12: Total number of GPS jamming events each day during the Christmas 2013 period

Note that there were no events on Christmas Day, Boxing Day or during the following weekend.

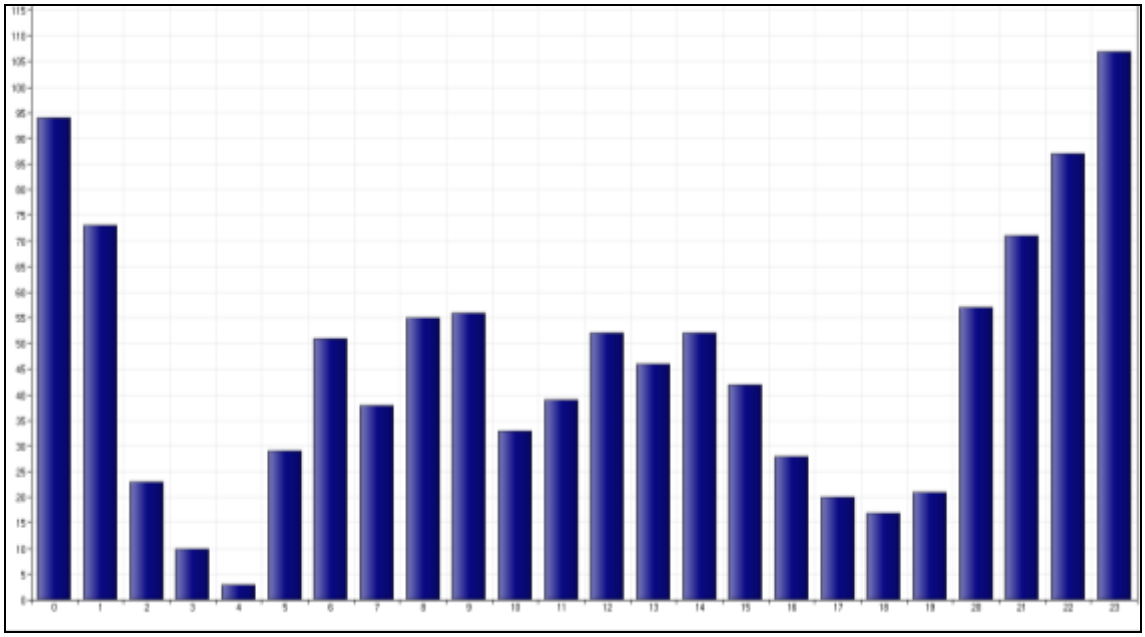

Figure 13: Totals of GPS jamming events in each hour of the day from February 2013 to December 2013

Note how different this pattern is from the record taken close to a motorway shown in Figure 9. The distribution of events here may be due to the large number of commercial service vehicles that enter the City of London at night, outside the congestion-charging period.

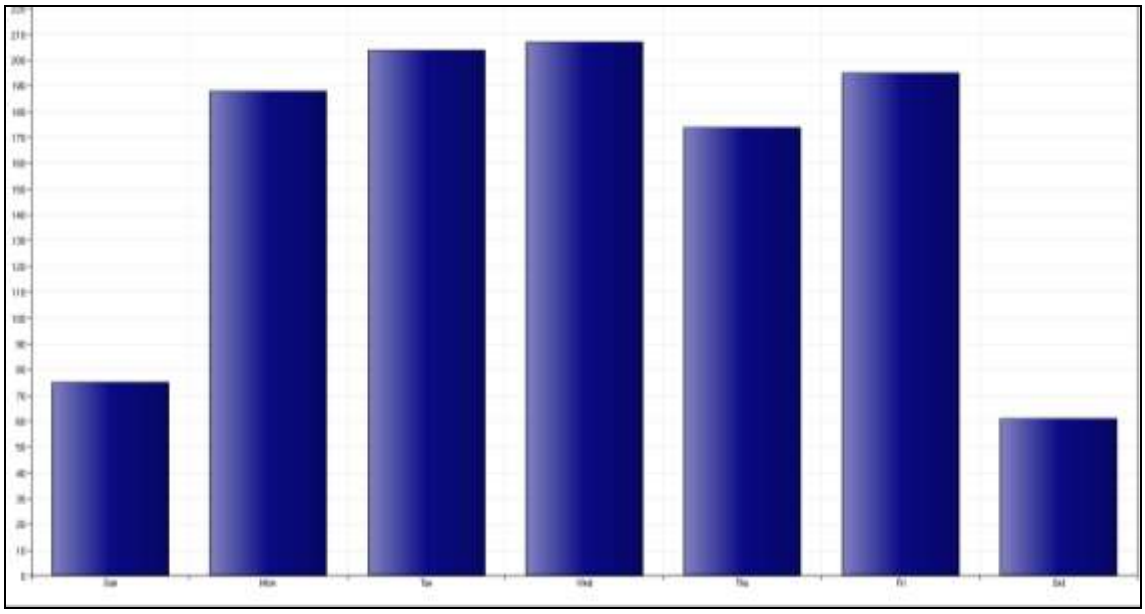

Figure 14: Totals of GPS jamming events on each day of the week from February 2013 to December 2013

The dominance of Monday to Friday events over weekend events suggests business use of jammers

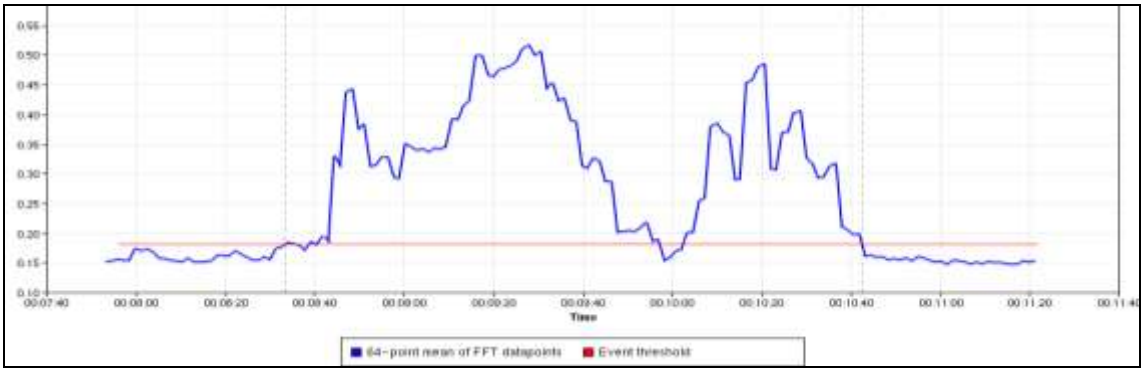

Figure 15: Time signature of a typical GPS jamming event at this site.

The strength of the received interfering signal is plotted over a period of approximately 160 seconds. The total duration of the double-peaked even is approximately 120 seconds.

4.5 WHO OR WHAT JAMS?

It is of course difficult to gather information that can reliably be used to attribute a jamming incident to a specific vehicle, individual or technology. Such evidence can best come from the seizure of a jamming device. Alternatively, an observer using a hand-held jammer detector at the road-side may be able to associate a jamming event unambiguously with the passage of a specific vehicle. There is little information to be gleaned from victims of GPS jamming; non-technical users are very unlikely to be in a position to attribute their loss of GPS service to jamming at all, never mind a specific jammer. Other classes of user, possibly including law-enforcement agencies, may be reluctant to admit to their vulnerability to jamming.

Over the course of the SENTINEL project, a significant amount of evidence has been built up that at least suggests what groups of drivers are principally responsible for jamming GPS. This can inform speculation as to the most likely motivations and applications of this jamming. Let us consider 5 categories of jamming: Nation State, Enemy, Terrorist, Criminal and Civilian as well as accidental jamming due to misbehaving technology.

4.6 NATION STATE & ENEMY JAMMING

4.6.1 NORTH KOREA JAMMING HITS SOUTH KOREA FLIGHTS

Jamming signals, believed to have been broadcast from North Korea, seriously affected GPS navigation on at least 250 flights in South Korea in April 2013. According to the South Korean transport ministry, the flights had to rely on alternative navigation systems. The GPS disruption affected Incheon international airport. The ministry did not attribute blame. However, previously in August 2010 and March 2011, South Korea had accused North Korea of conducting jamming attacks.

The GPS Jamming power was apparently quite considerable; some reports put it at 50 Watts - approximately 1000 times more power than is radiated by a typical hand-held jammer. This jamming was powerful enough to disrupt the mobile telephone network in Seoul, the capital of South Korea, 50 miles from the border. The network affected uses CDMA technology, a system in which each base station relies on its own GPS receiver for its precise timing.

4.7 TERRORIST JAMMING

The detection of Nation State, enemy and terrorist jamming is beyond the scope of this Report. However, the relevance of SENTINEL to these questions is evidenced by the Hansard record from the House of Lords.[3]

4.8 CRIMINAL JAMMING

4.8.1 VEHICLE AND HIGH-VALUE ASSET THEFT

The magazine "Fleet Directory" reported in April 2012 see Appendix A.29 that police in Kent had arrested and jailed members of a criminal gang responsible for the theft of some 150 Mercedes Sprinter vans over an 8 month period in the Heathrow Airport area. The gang had used jammers to disable tracking systems fitted to the vans to allow them to be tracked if stolen.

In 2013 a handheld jammer detector, developed within the SENTINEL Project, was loaned to a police force which used it in a training exercise. They simulated an attempt to recover items of capital plant equipped with GPS tracking devices after they had been stolen. The tracking devices indicated that their GPS reception was being interfered with by a "possible GPS blocking device". The handheld jammer detector successfully identified the presence of a jammer nearby on several occasions. However, by the time the stolen items had been recovered, the jammers had been removed.

The most popular style of GPS jammer employed by criminals, according to seizures by the police and OFCOM, are units of the 'cigarette lighter' style or multiband combined GPS and mobile phone jammers; examples of both types are illustrated in Section 7. Jammers like these radiate signals of relatively low power. It is common for advertisements for such jammers to underestimate their ranges. As Section 10 will show in more detail, trials conducted under controlled conditions on a military test range at Sennybridge, Powys demonstrated that such jammers can be detected by SENTINEL units at ranges of up to 250m.

There is evidence to suggest that jammers being used recently by organised criminals stealing high-value vehicles are more powerful than these small units; indeed jamming ranges of miles in open country are now possible. The increase in jamming power not only increases jamming range, but also helps offset the screening effect of metal bodywork on a jammer inside a vehicle; for example, a low-powered jammer plugged into a cigarette lighter socket inside a vehicle may not reliably block GPS reception at antenna on the roof outside the vehicle.

In the course of the SENTINEL project additional information concerning the use of GPS jammers by criminals has been gathered. Further details are available from Chronos Technology.

---

[3] Lords Hansard: http://www.theyworkforyou.com/wrans/?id=2011-03-16a.68.3

"Question** Asked by **Lord Patel of Blackburn
To ask Her Majesty's Government what steps they plan to take to reduce the vulnerability of global navigation satellite systems to terrorist attacks.

***The Minister of State, Home Office (Baroness Neville-Jones):** Global navigation satellite systems such as global positioning systems (GPS) are widely used within industry systems in the UK and have brought significant benefits to applications and services. There is substantial resilience across the systems including the availability of back-ups and use of alternative methods such as atomic clocks which helps to reduce over-reliance on GPS.*

The Centre for the Protection of National Infrastructure (CPNI) provides advice and guidance to organisations on protective security measures to reduce vulnerability to national security threats including terrorism. This includes advice on the use of space technologies such as GPS. CPNI also facilitates an information exchange which enables member organisations to share vulnerability information on space-derived services.

*Her Majesty's Government are taking steps to counter interference of GPS systems. These measures include **Project SENTINEL** which aims to provide the capability to detect and locate the source of GPS interference, warn critical users and enable law enforcement agencies to take action when criminal activity is involved. This project consists of a consortium which includes the Association of Chief Police Officers, the UK Space Agency, the National Physical Laboratory, the General Lighthouse Authority, Ordnance Survey, universities and the private sector."*

4.8.2 EVASION OF COVERT TRACKING

Law Enforcement Agencies (LEAs) routinely employ covert techniques to track the movements of suspects, especially those who may be engaged in organised crime. Internationally LEAs are aware of the use of GPS jammers by suspects to evade such means of detection. Further detailed information is beyond the scope of this report.

4.8.3 DEFEATING GPS BASED ELECTRONIC TAGGING

Electronic ankle tags are used to monitor persons who are under various forms of curfew. Increasingly, such tags are incorporating GPS receivers which report their measured positions to a control centre, usually via a mobile telephone data network. This form of monitoring is vulnerable to being defeated by the use of GPS jammers.

4.9 CIVILIAN JAMMING

4.9.1 AVOIDANCE OF FLEET TRACKING

Tracking systems for vehicles, especially those in commercial fleets, are now used widely. Costs have fallen to less than £100 per unit. Most employ a GPS receiver to measure the vehicle's position which is then reported at intervals via a mobile telephone data network to a control centre. Such tracking systems are highly vulnerable to GPS Jamming. They are also vulnerable to jammers which block their mobile phone data communications (see Section 7 below).

It is interesting to analyse the pattern of jamming events recorded by the SENTINEL unit at the site close to a motorway shown in Figure 7 & Figure 9 above. The pattern of events hour-by-hour through the day shown in Figure 8 is consistent with many of the jammers being deployed by the drivers of commercial vehicles in order to defeat such tracking systems. This is supported by extensive anecdotal evidence of the use of GPS jammers by "White-Van Men". The more than 1000 jamming events recorded at that site over a 12-month period broadly correlates with traffic densities and the pattern of movements of such drivers during their working day. There are very few events during the night.

4.9.1.1 Detection of a specific jammer during SENTINEL

One of the GAARDIAN partners was Ordnance Survey (OS). OS operates a network of differential GPS (DGPS) reference stations across the UK, some of which had been experiencing intermittent and unexplained temporary GPS receiver outages. It was decided to locate SENTINEL probes at a few such sites. One probe began recording events immediately upon installation. The University of Bath and Chronos Technology adjusted the parameters there to minimise the detection of false positives events caused by multipath propagation (see Section 4.2 above). Jamming events continued to be detected, as shown in Figure 16Figure 18 below.

Details of these events were shared with local Law Enforcement Agencies (LEA) who analysed the data. This exercise was undertaken manually by the LEA team before a graphical "Event Analysis" feature was added to the SENTINEL Server. Now we can recreate this exercise more easily on-line: some of the results are reproduced in Figure 16Figure 18 below.

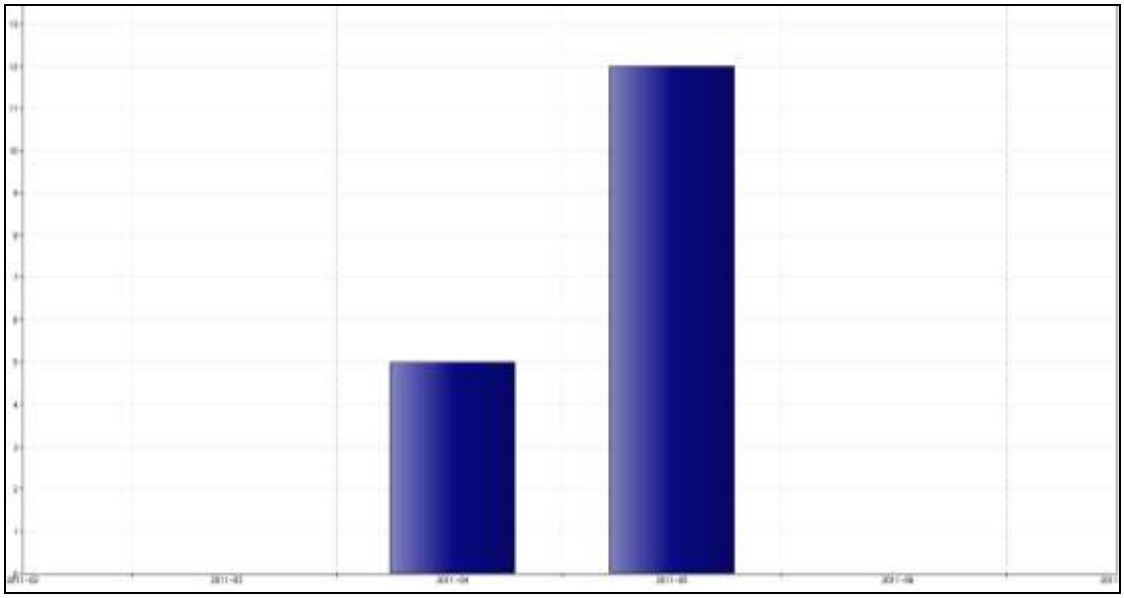

Figure 16: Total number of GPS jamming events detected in April 2011 and May 2011.

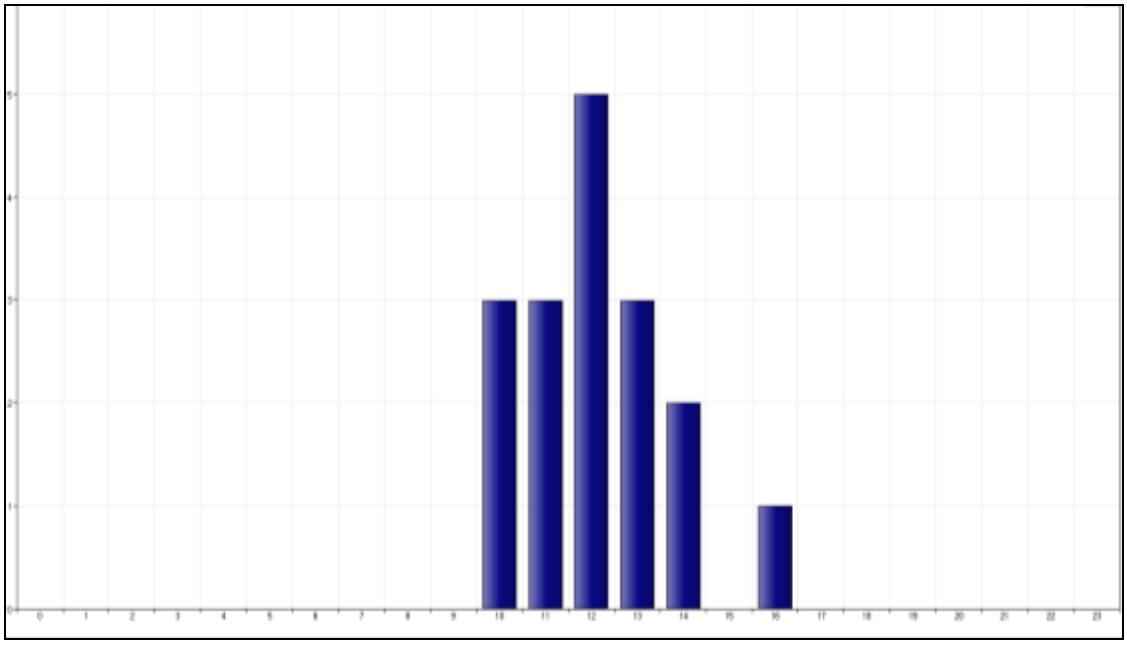

Figure 17: Totals of GPS jamming events detected in each hour of the day in April 2011 and May 2011.

Note the absence of night-time events at this site.

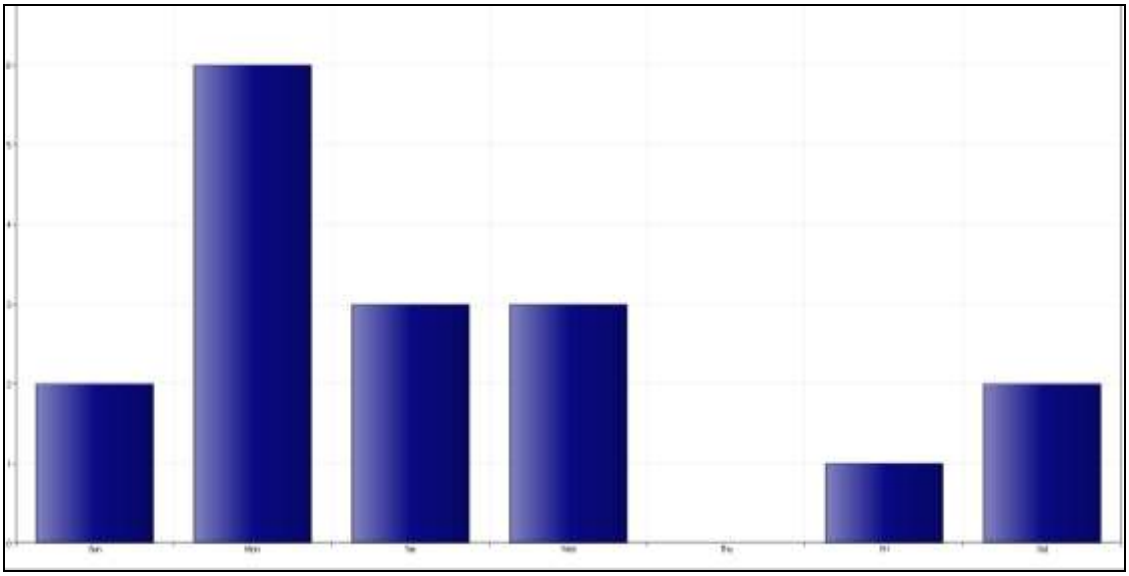

Figure 18: Totals of GPS jamming events detected on each day of the week in April 2011 and May 2011

From this intelligence it became clear that there was a pattern: jamming events were most frequent on Mondays around midday. Details of the ensuing LEA operation are restricted but we can report that a handheld jamming detector (a predecessor of the CTL3510 GPS Jammer Detector described in Section 8.1.1 below) associated the jamming with a GPS jamming device of the GP5000 type (see Section 6.1.1.2 below) carried in a company fleet vehicle. It was discovered that the driver was seeking to defeat his employer's vehicle tracking system.

This was a clear breakthrough for the SENTINEL project. It demonstrated that, given appropriate actionable intelligence, LEAs can track down GPS Jammers in matter of weeks. The LEA handed the jammer they seized to the SENTINEL team who tested it during trials at Sennybridge (see Section 10 below). The results thus contributed to the SENTINEL programme.

This rapid and successful response to the detection of a jammer within 3 weeks may be contrasted with the 6 months required to apprehend the perpetrator of the Newark jamming incident described in Section 4.9.1.2 below.

More details relating to this operation can be found in the Chronos white paper "Protecting the UK Infrastructure: A System to Detect GNSS Jamming and Interference"[4].

4.9.1.2 The Newark Incident

The "Newark Incident" has done more to publicise the vulnerability to GPS jammers of mission-critical and safety-critical services than any other event. It took the US Federal Communications Commission (FCC) and Federal Bureau of Investigation (FBI) some 6 months to determine the cause and track down the perpetrator. The Fox report in APPENDIX C C.3 describes the case and the press report described in the www.liveviewgps.com blog[5]:

"GPS jammers are illegal in the United States because of their ability to block important communications. For one New Jersey man, the cost was much higher than he anticipated.

Gary Bojczak first got the jammer to block his employer from tracking his whereabouts during his work shift. The company he worked for installed GPS tracking devices on all work trucks, including the one he was

[4] "Protecting the UK Infrastructure: A System to Detect GNSS Jamming and Interference" available via this link
[5] http://www.liveviewgps.com/blog/employee-fined-32000-gps-jammer/

driving. They did this in order to monitor the trucks' location and other data, and be sure company time was being used wisely.

Unfortunately for Bojczak, using the signal jammer device also blocked a nearby GPS system that was being used at Newark Liberty International Airport, where they were attempting to test a new GPS system for their plane routes. As Bojczak pulled up next to the airport on his route, the GPS system was jammed, which alerted the airport's security team.

Security was able to trace the issue back to the Ford pickup truck that Bojczak was driving. They investigated the matter further, along with one of the agents from the Federal Communications Commission (FCC).

It didn't take too long to discover that Gary Bojczak, an engineer, had used a GPS jamming device to block communications from his truck's GPS tracking system. He was then charged with interfering with authorized communications, since it is against the law in the U.S.

In the case of Gary Bojczak, he was charged with the offense and received a $32,000 fine for obtaining and using the jamming device. The FCC considers the fact that they caught him in time lucky, because they have had many crossed signals due to jammers and never find their operators."

4.9.2 COMMERCIAL ADVANTAGE

"Taxi cheats using GPS Jammers to steal fares"

In November 2013 a Melbourne newspaper, the Herald Sun[6], reported as follows:

"… dozens of Melbourne cabbies suspected of using GPS jammers had been reprimanded, or given their marching orders by one taxi booking network.

Communications authorities warned that devices are a potential risk to public safety as they can obscure the location of police cars, ambulances and fire trucks. The contraband jammers can disguise the location of taxis by disrupting satellite navigation system signals.

Drivers had been caught using them in order to fool cab companies into giving them jobs even though they were not in the area. Several jammers were confiscated.

13 CABS chief operating officer Stuart Overell said the booking network had kicked out or admonished more than 100 drivers since it introduced technology to detect jammers early last year.

The executive manager of the operations and services branch of the Australian Communications and Media Authority, Mark Loney, said: "Jammers put people at risk, as they can prevent legitimate signals from getting through. It's like a bad traffic jam," he said. He added "If one of these jammers is switched on when within a few car lengths of a police car, there's a danger that the police dispatch centre may have an incorrect location for the police car,'' Mr Loney said. "Also, if the taxi was involved in an accident, the taxi dispatch centre may also have a wrong location for that vehicle.''

Staff from ACMA and the taxi industry regulator, armed with radio emissions detectors, conducted a sting operation, dubbed Operation Signal, at city taxi ranks for several months early this year. As a result two drivers were charged with breaking the Radio communications Act by "engaging in conduct which results in substantial interference or substantial disruption or disturbance with radio communications".

They are due to face magistrates' courts next month on the charge, which carries a maximum penalty of a year's jail."

How did this GPS jamming work?

[6] http://www.heraldsun.com.au/news/law-order/taxi-cheats-using-gps-jammers-to-steal-fares/story-fni0fee2-1226756138559

A cabbie would switch on the jammer. The jammer disguises the taxi's true location and gives the impression the cabbie is in a certain suburb or area for a long time waiting for a fare, when in fact they are actually out getting other fares. Booking networks then offer the next fare in that suburb or area to the cab driver, thinking they have been waiting the longest. The driver who has actually been in the suburb or area the longest misses out on the fare

4.9.3 ACCIDENTAL UNINTENDED CONSEQUENCE TO GNSS OF CELLULAR JAMMING

Accidental jamming of GPS as an unintended consequence of using a combined GPS/mobile phone jammer to block mobile phones. For example cell phone jammers have been advertised by companies that offer "off-site meeting security services". If these were the combined GPS/Mobile phone jammer variety as illustrated in Section 7, this would cause localised jamming of GPS.

This unintended consequence provides two amusing anecdotes that illustrate the important truth that jamming carried out with good intentions may impact critical GPS applications.

4.9.3.1 "The Priest and the Jammer"

In a presentation at CGSIC 2012 in Nashville[7] an official with a US Government Agency bought handheld GPS jammer detectors from Chronos Technology during the SENTINEL project. A colleague, who had one with him when he attended church on Sunday, was surprised when it was activated. When he made enquiries, the priest proudly showed him his new jammer, remarking how effective it was in stopping cell-phones from ringing during his sermons!

4.9.3.2 "The Quiet Carriage Traveller"

A UK government employee was travelling home from London by train. He sat in a "Quiet" carriage, in which passengers are asked not to use mobile phones, a request widely ignored. He met there a friend who proudly showed him his new "gadget" which solved the problem: a GPS/mobile phone jammer!

4.10 SPOOFING

Spoofing is the transmitting of false GPS signals by means of which the perpetrator commandeers a GPS receiver, causing it to indicate positions and apparently follow journeys of his choosing. Examples are given in APPENDIX C particularly the references to Prof. Todd Humphreys' experiments.

Chronos conducted experiments during the SENTINEL project with Coherent Navigation's GPS Phase-Coherent Simulator and its ability to change the time delivered from the GPS receiver without the receiver going into alarm mode.

Figure 19 below shows how a timing receiver can have its time spoofed. The test shows the time being pulled at a rate of 300 µsec every 5 minutes. During this test the GPS receiver did not go into alarm.

[7] CGSIC 2012 Nashville http://www.ion.org/gnss/upload/GNSS12Program.pdf

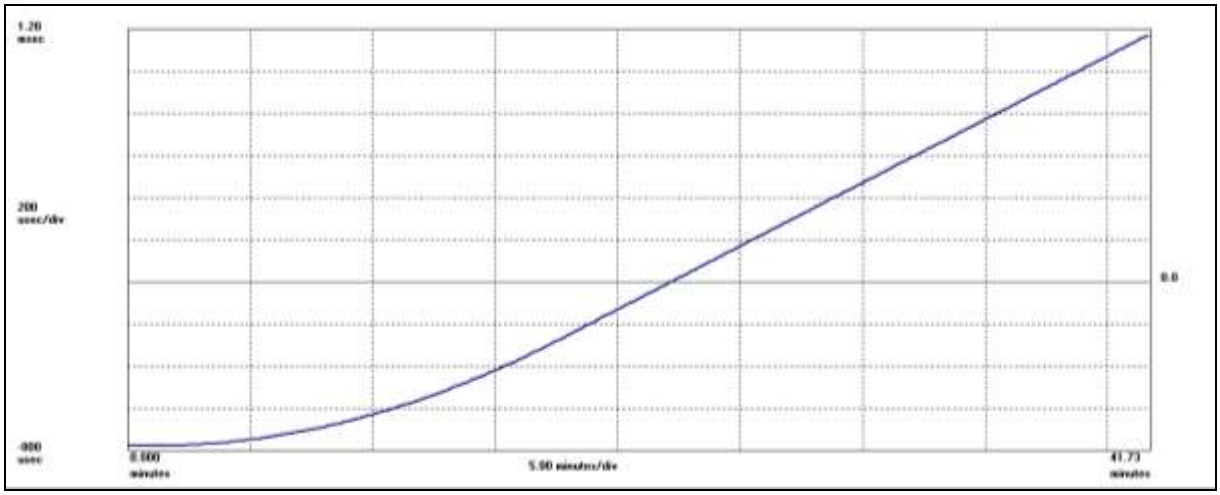

Figure 19: Timing Receiver under spoofing attack

4.11 REBROADCASTING ANTENNA

Occasionally, GPS antennas which have been deployed for many years can exhibit a fault condition where they rebroadcast the GPS signal. This rebroadcasted signal will have been amplified by the first stage of gain in the antenna and reflected back out due to an impedance mismatch.
This, quite effectively, denies GPS reception in the vicinity of the GPS antenna and in one instance attended by Chronos support staff recently - Figure 20, succeeded in denying nearby GPS reception at a radius of at least 30m from the reradiating antenna.

Figure 20: Rooftop location of reradiating (red) and victim (blue) antenna.

The picture on the right shows the CTL3500 Jamming detector (a predecessor to the CTL3510 described in Section 8.1.1) indicating significant jamming power.

5 APPLICATIONS VULNERABLE TO GPS JAMMING AND SPOOFING

The dependence of our society on GPS (and, increasingly, on GNSS systems in general) is significant and in many cases they are essential to our daily lives. Critical areas of public infrastructure include the Airwave (Tetra) communications network used by the emergency services and the National Grid. This network, and many other systems, depend on the reliable operation of GPS receivers, and our dependency is growing. Since criminals and terrorists are aware of this vulnerability, there is an increased probability of intentional interference with GPS signals – especially given the ready availability of commercial jamming devices. Their

economic impact is likely to be significant; so too will be the requirement for funding means of mitigating the problem by identifying and locating sources of interference precisely and reliably. Of course, this is a global problem; certainly other EU countries are becoming increasingly concerned about GNSS interference and the need for solutions.

5.1 GBAS, SBAS, EGNOS & WAAS AIRCRAFT LANDING SYSTEMS

One of the first applications to admit to a vulnerability to GPS Jamming was a trial aircraft instrument landing system at Newark International Airport in the US that employs a new Ground-Based Augmentation System (GBAS) technology; the series of jamming events that interrupted its operation was mentioned in Section 4.9.1.2 above.

The perpetrator, who used a plug-in cigarette lighter-style jammer of low power, travelled routinely along Highway I95 which runs past the Airport. The GBAS antenna that receives GPS signals was just inside the perimeter fence, where the interference was very strong when the vehicle was passing. The immediate mitigation solution was to move the antenna further into the airport complex. That solution would have been unlikely to succeed had a higher-powered jammer such as the J242-G J model (See Section 6.1.1.3) been employed.

Conversations with aeronautical organisations that employ other GNSS technologies for aircraft landing systems, including Space-Based Augmentation Systems (SBAS), confirm that they too are concerned about GPS jamming. They are also aware of the vulnerability of the Wide Area Augmentation System (WAAS) and its European equivalent the European Geostationary Navigation Overlay Service (EGNOS), both of which play key roles in ensuring the integrity of GNSS-based aeronautical navigation systems.

5.2 WIRELINE TELECOMMUNICATIONS NETWORKS

Wireline telecommunications networks have been using GPS signals as a source of precise timing since 1996. Upon the loss of GPS signals they maintain synchronisation by reverting automatically to built-in "holdover" sources of time, previously synchronised to GPS, that employ high-stability Oven-Controlled Crystal Oscillators (OCXO) or Rubidium atomic clocks. Additional mitigation of the effect of loss of GPS is provided by taking timing from a Caesium atomic Primary Reference Clock (PRC), communicated over the network itself. One means of communication is over the Ethernet systems increasingly used by telecom networks; the International Telecommunication Union (ITU) through its Standards Study Group 15, Question 13 has adapted the IEEE 1588 Precision Time Protocol (PTP) for this purpose. Given these fall-backs, wireline telecommunications networks, if architected appropriately are generally resilient to GPS outages.

5.3 WIRELESS TELECOM NETWORKS

Currently, Frequency Division Duplex (FDD) wireless telecom networks require frequency references of only 1 part per billion, a relatively low accuracy. However, the incoming generation of 4G networks will use Time Division Duplex (TDD) techniques which require sub-microsecond time accuracy. The new services and capabilities carried over these networks, such as Coordinated Multipoint (CoMP) in which a handset may communicate with a macro site and a small cell site simultaneously, will need a timing source with an accuracy of 500ns, and this at the edge of the network. Some organisations are providing this by using GPS alone, as is currently the case with Code Division Multiple Access (CDMA) networks.

The vulnerability to the loss of GPS of this approach was clearly to be seen during jamming attacks the by North Korea on South Korea (see Section 4.6.1): numerous CDMA mobile phone sites lost their timing and failed. A similar loss of cells was seen in the US in 2007 when a warship in San Diego harbour accidentally jammed GPS signals in the city, causing parts of the city's networks to shut down for up to 3 hours.

5.4 ELECTRICITY GENERATION AND SUPPLY

The Electricity Generation and Supply industry requires sources of timing accurate to better than 1 microsecond for fault tracking and phase alignment. Increasingly, this timing is supplied by GPS receivers.

The systems employed have far less resilience than do telecommunications networks and GPS installations are sometimes of a low standard.

This industry admits it has vulnerabilities but has devoted little effort to mitigating or deterring interference since, so far, no problems have been attributed to GPS Jamming.

5.5 FINANCIAL TRADING

A recent UK Government report[8] recommends that financial trading systems should use GPS for their synchronisation, since an accuracy of better than 1 microsecond is required. Because this approach will render such systems vulnerable to sustained GPS jamming attacks, mitigation techniques should be identified and implemented.

5.6 TELEMATICS INSURANCE

Telematics insurance is a relatively new, but rapidly-growing, form of motor insurance. It has proved a viable solution to the challenge of reducing the very high cost of the premiums for new drivers. The vehicle carries a telematics unit which monitors the driver's journeys and driving style, allowing premiums to be adapted to risk. The on-board telematics unit also provides detailed data on any collisions. This technology is wholly dependent on GPS reception on the vehicle and so vulnerable to the use of GPS jammers.

5.7 TRACKING OF ASSETS, FLEET VEHICLES & PEOPLE

GPS-based tracking solutions are becoming a commodity offering: one unit has just come onto the market priced at £99.99 with 28p per day of all costs and support. Many of these systems have no protection whatsoever from GPS jamming. Others employ hybrid solutions, with at least some input from accelerometers or other sensors independent of GPS to provide continuity of operation, albeit for limited periods and distances only.

There is already clear evidence from Law Enforcement Agencies that GPS jammers are being used to assist in the theft of high-value assets.

5.8 ROAD USER CHARGING

GPS-based Road User Charging is potentially big business. Whilst it is not currently in use in the UK there is an annual conference[9] focusing on the market.

There is already clear evidence of GPS Jammers being used where road user charging schemes have been deployed; they defeat what some people consider to be a form of taxation.

5.9 UNMANNED ROAD VEHICLES

Experiments with unmanned road vehicles have been conducted by the US Institute of Navigation (ION) which runs an annual competition in which teams from academic institutions race unmanned vehicles over 200 miles of desert or navigate around cities. Google and Amazon are developing unmanned cars and drones. They all use GPS.

There have recently been successful demonstrations of the vulnerability of unmanned aircraft and ships to GPS spoofing attacks. See APPENDIX C.

5.10 GEOFENCED APPLICATIONS

Cash-in-transit services widely use GPS-based geo-fencing techniques: the doors of their vehicles are locked until a GPS receiver indicates that the vehicle is in a location where opening them is permitted.

[8] UK Government Office for Science Report "The Future of Computer Trading in Financial Markets"

[9] Road User Charging Conference 2014, Belgium http://roaduserchargingconference.co.uk/

Such systems are vulnerable to jamming and spoofing attacks.

6 JAMMERS, JAMMER TYPES & WHERE THEY COME FROM

In the course of the SENTINEL project a survey of web sites has been undertaken in order to determine the availability of GPS jammers on sale over the Internet. Specification details were recorded. Jammers were then purchased to allow the service to be assessed.

On the whole the experience was similar to that at any on-line shop. However the commercial invoice accompanying the consignment would generally identify the contents not as a "Jammer" but as, for example, a "Router" or "Charger". A typical jammer is supplied from Hong Kong and costs less than USD100, including shipping.

The following sections review jammers acquired in this way and others seized by LEAs or OFCOM.

6.1 TYPES OF JAMMERS

Commercial jammers come in many types, shapes, sizes and capabilities. Most fall into two categories: GPS-only; and GPS combined with mobile communications. There are also jammers that target WiFi, Bluetooth or CCTV frequencies; these are not reviewed here. There appears to be a tendency for commercial jammers to become more sophisticated and more powerful.

The following is not an exhaustive list of jammers. Instead it presents examples, all obtained in the course of the SENTINEL project. These jammers have been tested to determine the ranges over which they affect GPS receivers, and the ranges over which they can be detected. Testing took place during the Sennybridge trials see Section 10.1 using 24x7 sensors described in Section 8.2.1 and handheld detectors similar to the ones described in Section 8.1.

6.1.1 GPS-ONLY JAMMERS

The first GPS-only jammers operated at the L1 frequency used by civil GPS receivers. They were principally of two types: cigarette-lighter-style (see example on page 30); or rectangular hand-held units with internal batteries (see Figure 21 below). Most jammers generate chirp (that is frequency-swept) transmissions by means of a timer chip of the family known as '555'. This sweeps the frequency of the radio transmission from the jammer across L1 frequency band. It is suspected that this technique has been adopted to ensure that transmissions do actually cover the L1 band despite the low accuracy of the Temperature Compensated Crystal Oscillator frequency sources employed. Recent designs are not only of higher power, but also are designed to cover all frequencies of the new GPS transmissions and all those of other GNSS including Galileo; that is, they block the frequency bands known as L1, L2, L3, L4 and L5.

6.1.1.1 J220-C

The device shown in Figure 21 is found on many websites, variously marked J220-C, TG1002, EJ305, GJ02 or J1000. A similar unit, called the 808KB has the antenna offset and the on/off switch on the top rather than on the side. It transmits 200mW (ie 23dBm) in the L1 band only. It employs an internal battery and is supplied with a charger device for mains or car use. It weighs 37g and its dimensions are 95×48×18 mm.

Figure 21: J220-C GPS Only Jammer

At the time of writing, such units were priced on one web site at $51. It can also be found as an OEM PCB assembly with model number 110C, priced at $24.10.

Some advertisements claim an effective range of 10m. In practice the jamming range was found to be much greater, but would be dependent on the sensitivity and vulnerability of the victim receiver. The detection range was at least 200m depending on terrain and building shadowing.

6.1.1.2 GP5000

This device is found on many websites, variously marked GP5000, GJ5000, GJ01, JYT-GP04 or EJ308. It transmits 130mW (21dBm) in the L1 band only, works off the 12V cigarette lighter, or auxilliary power, socket in a vehicle. It weighs 35g and has dimensions of 80x21x21mm.

At the time of writing, this unit was priced on one website at $14.75 – and on another at $498!

It is openly advertised as being able to defeat "Verizon Fleet Administrator", "OnStar Family Link" and "Track What Matters" systems.

This device appears identical to the one seized in the exercise reported in Section 4.9.1.1 above. It claims an effective range of 5m. Its measured range was much larger and the unit was detectable at even greater distances.

6.1.1.3 J242-G

Figure 22: J242-G Jammer

This device, variously known as the J242-G, WF-121G, TG-121G or JYT-GP03, is by far the most sophisticated GNSS-only device we found. Rated at 0 .5W (27dBm) per channel of four channels, it covers the L1, L2, L3, L4 and L5 GNSS bands. It claims to be the first jammer to target all GNSS bands. Specifically these are GPS L1: 1500-1600MHz, GPS L2: 1220-1230MHz, GPS L3: 1200-1210MHz, GPS L4: 1250-1280MHz, GPS L5: 1170-1180MHz. L2 and L3 share a channel.

This device jams not only GPS, but also Galileo and Compass, plus the WAAS, EGNOS, QZSS and GAGAN augmentation systems. With Galileo, it blocks not only normal civil Galileo but also the Public Regulated Service (PRS) intended for government use. When all 4 channels are switched on simultaneously, the multiple intermodulation products interfere with GSM and CDMA bands, apparently unintentionally. Whilst it does not cover all of the current GLONASS band it will block the proposed future GLONASS transmissions on the GPS L1 frequency. It claims a range of 15m but tests have shown it is detectable depending on terrain at up to a few miles.

The device weighs 275g, with dimensions 113×60×30mm. It has an internal battery and is supplied with a charger device for mains and car. It also comes with a leather pouch and belt clip.

At the time of writing, this unit was priced on one web site at $187. The invoice described it as a 'Router', of value '$20'.

Recently a similar unit – the J-240D rated at 2.7W covering L1 and L2 was seized by police during a raid. This is an interesting development. Whereas "White-Van" Man is using the low cost cigarette lighter style unit, organised crime prefers the more powerful battery operated devices.

6.1.2 JAMMERS FOR GPS PLUS MOBILE PHONES

The purpose of devices of this type is to block both GPS and local mobile phone signals simultaneously. This is of particular value for those who wish to attack tracking systems.

6.1.2.1 J220-B

Figure 23: J220-B GPS & GSM Jammer

This device, the J-220B, transmits at 850-960MHz (GSM phones), 1805-1990MHz (DCS phones) and 1500-1600MHz (GPS L1). There is also a version for US mobile phone frequencies. It transmits 130mW (21dBm) in the GPS band, has an internal battery and is supplied with a charger device for mains and car. It weighs 37g and with dimensions 95×48×18 mm.

The jamming radius for GPS is stated to be "up to 20m". Depending on the GPS receiver, it can jam at a much greater range than this and was detectable at 250m.

This unit can also be found as an OEM PCBA with model number 110B, priced at $23.40

6.2 JAMMER WEBSITES

Many of the websites that sell jammers are ephemeral; others, permanent. APPENDIX B lists websites active at the time of writing. During the project over 100 sites have been identified, mostly based in China. At the time of writing this report, about 40 are currently active. One is in the Ukraine. Chinese sites can only be accessed from outside the country. Some UK sites and eBay sellers have been shut down by OFCOM.

7 MITIGATION

The overall conclusion from this Report is that GNSS signals are vulnerable to jamming. Jamming is not going away; in fact, jammers are becoming more numerous and more powerful.

A report such as this on GNSS Vulnerabilities would not be complete without its examining some of the solutions that are emerging to mitigate the threat to PNT. This has been a key feature of SENTINEL, as it was for GAARDIAN before it. Let us review some approaches to mitigation.

7.1 MITIGATION TECHNIQUES

7.1.1 RESILIENT TIMING

A recent paper[10] see Section 13 reviews the various ways of building resilience into timing equipment by synchronising to GPS various kinds of clock which thereafter have the ability to remain accurate during periods of GPS loss of various durations. Existing techniques include the use of Oven Controlled Crystal Oscillators (OCXO), Rubidium atomic clocks and the new Chip Scale Atomic Clocks (CSAC).

Time and timing can also be transferred around telecommunications networks by means of the techniques reported in Section 5.2 above and found on the ITU web site here.

[10] Dependency of Communications Systems on PNT Technology

7.1.2 GPS ANTENNA TECHNOLOGIES

Figure 24: GPS Antenna "Squatters"

Whilst short-term relief from GPS jamming can be attained by moving the GPS receiving antenna further from the source of interference – See Section 4.9.1.2. There is no accounting for what may happen from 3rd party activity in the vicinity of a GPS antenna installation. Chronos has had experience of antenna "squatting" where, for example, lazy installation engineers will use the GPS antenna pole to fix another GPS antenna or one for a completely different technology such as a microwave radio link. See Figure 24. There is so much evidence of complete disregard for GPS antenna installation best practice that Chronos has now published an Application Note[11].

An alternative approach is the use of GPS receiving antennas, the horizontal radiation patterns of which have been designed to have one or more deep nulls, capable of being steered in azimuth. A null is pointed directly towards any source of interference detected. These antennas are known as Controlled Radiation Pattern Antennas (CRPA). This technology is widely employed by military users but is still too expensive or cumbersome for most civil markets. Tests have been conducted within the SENTINEL Project – see Section 8.3.2.

7.1.3 USE OF MULTIPLE FREQUENCIES

When GPS jammers used to target the L1 civil signal only, the use of the additional frequencies being embodied in the later versions of GPS appeared a promising method for mitigating the jamming threat. However, this has no longer been the case since multiband jammers which target all GPS frequencies, such as the J242-G device shown in Section 6.1.1.3, have now emerged.

7.1.4 USE OF MULTIPLE GNSS

As with the use of multiple frequencies, the ability to mitigate the threat of GPS jamming by switching to alternative GNSS, has been nullified by the appearance of jammers which cover all the frequency bands the various systems employ. All GNSS, with the limited exception of the current version of the Russian GLONASS system, use essentially the same frequency bands and so may be vulnerable to the same jammers.

7.1.5 ENHANCED LORAN (ELORAN)

Figure 25: Anthorn eLoran Transmitter

The General Lighthouse Authorities of the UK and Ireland (GLA), supported by the UK Department for Transport (DfT) have been providing a prototype eLoran trial service since 2007. See more information here. The first eLoran transmitter in the UK is situated at Anthorn radio station in Cumbria.

[11] GPS Antenna Installations. Best Practice

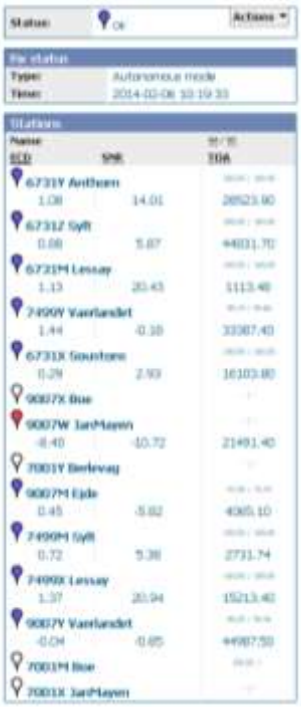

Figure 26: eLoran Stations

Each Loran station is equipped with a suite of specialized equipment to generate precise timing signals that modulate the powerful carrier wave they transmit. Their signals are precisely synchronised to UTC, using up to three commercial caesium atomic clocks which are adjusted to follow UTC (Brest) by a Control Centre in France that monitors the transmitted signals.

The quality of the Anthorn transmission was monitored throughout both the GAARDIAN and the SENTINEL projects. In particular, the timing stability and synchronisation of $eLoran_{UTC}$ was compared to GPS_{UTC} ($USNO_{UTC}$) within the SENTINEL Sensors and also at the National Physical Laboratory (NPL).
The record of Quality of Service (QoS) and timing stability data were (and remain) continuously available from the SENTINEL Server.

An eLoran Receiver will automatically track all transmitters it can receive. Figure 27: ECD, SNR and TOA Data from the Anthorn station plotted over 48 hours shows an example of such data which includes the Envelope-to-Cycle Difference (ECD), the Signal-to-Noise Ratio (SNR) and the Time-of-Arrival (TOA) readings for each station in range.

Since, as a source of precise timing, an eLoran receiver only requires the signals from a single station, eLoran is highly resilient to the loss of any one transmitter. A timing receiver, with the ability to switch between Loran stations whilst maintaining phase coherence, was developed and successfully demonstrated during the SENTINEL project.

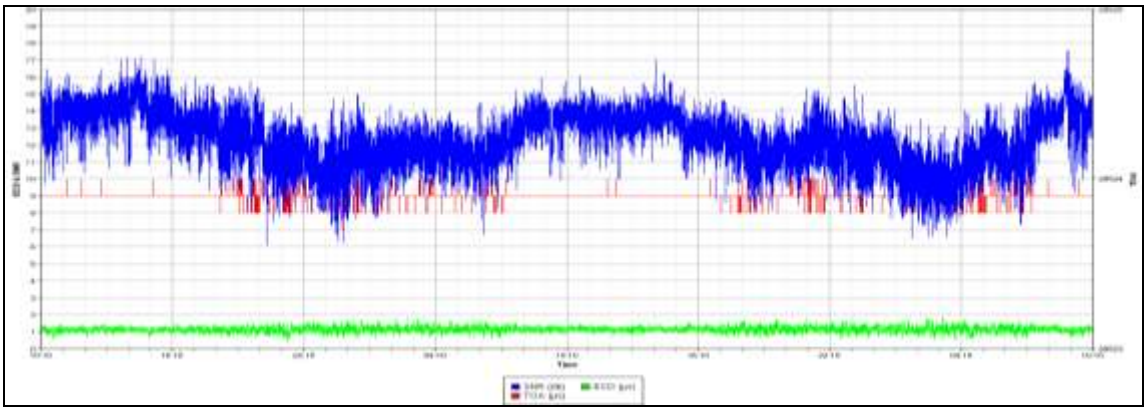

Figure 27: ECD, SNR and TOA Data from the Anthorn station plotted over 48 hours

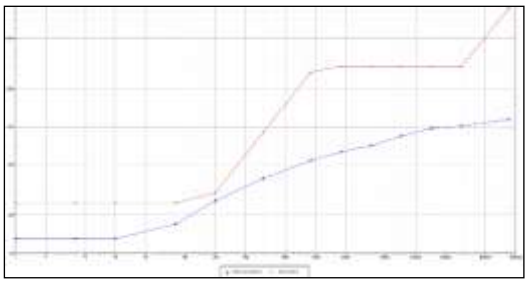

Figure 28: Relative MTIE between GPS and eLoran

A metric of great importance in assessing the quality of a timing receiver is “MTIE”, as defined in ITU standards for telecom timing. MTIE is derived by sliding windows of different observation interval through the datasets and plotting the resulting Maximum Time Interval Error (MTIE) data points on a log-log graph. In Figure 28, the red trace represents the ITU G.811 Standard for a Primary Reference Clock (PRC). The blue trace shows the relative MTIE between UTC taken from GPS and UTC from an eLoran source. The data comes from the SENTINEL Server GUI.

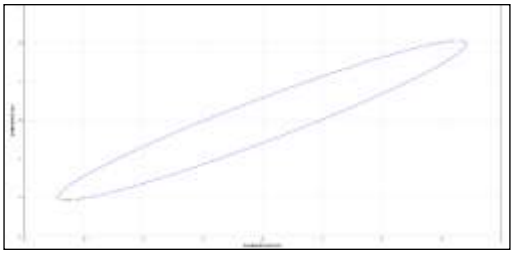

Figure 29: GLA QoS Display

The GLAs developed an algorithm that determines the QoS of position measurements made using eLoran. Figure 29 shows the error ellipse for the Anthorn signal as received at the Chronos Technology offices in the UK. There is a latitude error range of +/-~2m on the Y-axis and a longitude error range of +/-~3m on the X-axis.

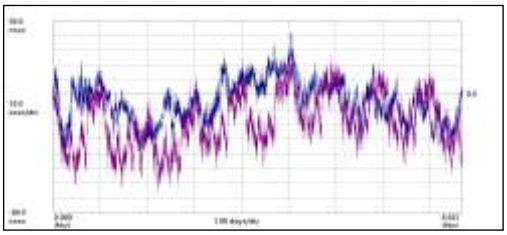

Figure 30: eLoran (Blue) and GPS (Magenta) TIE Graphs.

An example of the long-term relative GPS and eLoran timing performance is shown here in the Time Interval error (TIE) and Maximum Time Interval Error (MTIE) graphs. The blue trace is the eLoran signal and the magenta trace the GPS signal. The data was captured using test equipment independent of the SENTINEL monitoring system over a 9-day period during the Christmas break in 2013. The reference source was a Symmetricom 5071 Caesium oscillator, the offset of which had been normalised to zero.

The overall conclusion from this test and from monitoring eLoran signals during GAARDIAN and SENTINEL is that $eLoran_{UTC}$ is aligned to GPS_{UTC} ($USNO_{UTC}$), but independent of GPS. eLoran is a perfectly acceptable source of precise timing for telecommunications use, in particular the next generation of LTE TDD services and thus forms a viable mitigation in place of GPS in case of jamming.

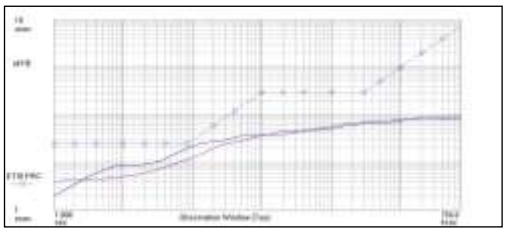

Figure 31 : eLoran (Blue) and GPS (Magenta) MTIE Graphs

7.2 LEGISLATION AND PROSECUTION

Legislation controlling the use of jammers varies from country to country; in many countries is still being developed. In the UK it is not illegal to possess a jammer although it is illegal to use it. Even if the law were changed to make possession an offence, it is unlikely that criminals or terrorists would be deterred. Indeed, reading the blogs from satisfied customers (see Appendix B.1), one wonders whether many have ever considered the question of legality!

8 EXPLOITATION ACTIVITY - JAMMING DETECTION SOLUTIONS

A key requirement of Technology Strategy Board research funding is a clear exploitation plan. In accordance with this plan, a number of jamming detectors for different applications been developed in the course of the SENTINEL project. These include hand-held units, jammer detectors and network-connected remote sensors. Some of these have now become full products. They are built in the UK and marketed globally through a network of international channels and OEM partners.

8.1 HAND-HELD JAMMING DETECTORS

Two hand-held devices have been created within the context of SENTINEL by the University of Bath. These have been fully field-trialled and commercialised by Chronos Technology. The CTL3510 is a simple battery-operated device. The CTL3520 has a unique capability to determine the direction in which the jammer lies.

Key features of the two devices are summarised in Sections 8.1.1 and 8.1.2.

8.1.1 CTL3510 GPS JAMMER DETECTOR

Figure 32: CTL3510 Jamming Detector

The CTL3510 GPS Jammer Detector is a low cost, hand-held, battery-operated device designed to detect the presence of GPS jamming or too much power or interference from any source in the GPS (L1) band. It is ideal for detecting commercially-available GPS jammers hidden in vehicles. A time-stamped event logging option enables covert deployment in vehicles where the driver is suspected of using a GPS Jammer.

Detection and location of GPS jammers in:
Any vehicle or human carrier
Multi-storey car parks
Taxi ranks at railway stations, airports etc.
Truck holding areas
Van depot gates
Ports, freight & container terminals

Key Features Include:

- Simple to use
- Detecting GPS jamming at 1575.42 MHz (GPS - L1)
- Visual LED display of jammer strength
- Vibrate alert
- Hand held - small size, light weight
- Rechargeable battery via micro USB with Low battery indicator

Users Include:

- Law Enforcement Agencies
- Communications Licensing Regulators
- Security Operatives
- Fleet Operators
- Critical Infrastructure Operators
- GPS Installation Engineers

The CTL3510 data sheet is available here.

The CTL3510 has an active plan for enhancements which will result in new features and products during 2014 and beyond.

8.1.2 CTL3520 GPS JAMMER DETECTOR AND LOCATOR

Figure 33: CTL3520 Jamming Detector and Locator

The CTL3520 GPS Jammer Detector and Locator is a hand-held, battery-operated device designed to detect and quickly locate jamming signals from commercially-available GPS jammers or too much power or interference broadcast in the GPS (L1) band. Ideal for the detection and location of GPS jammers hidden in vehicles.

Key Features:

- Simple to use
- Detecting and pinpointing GPS jamming at 1575.42 MHz (GPS - L1)
- High sensitivity
- Visual LCD & LED display of jammer strength
- Audio indication of jammer strength
- Hand held - small size, light weight
- Rechargeable battery via micro USB
- Battery Low indicator

Figure 34: CTL3520 in use

Users Include:

- Law Enforcement Agencies
- Communications Licensing Regulators
- Security Operatives
- Fleet Operators

The CTL3520 data sheet is available here.

The CTL3520 has an active roadmap which will result in new features and products during 2014 and beyond.

8.2 24X7 REMOTE-NETWORKED JAMMING DETECTION

A number of remote sensor solutions have evolved in the course of the SENTINEL project. Three of these address the GPS jamming threat specifically; the fourth is a proof-of-concept eLoran test platform for comparing eLoran UTC with GPS UTC. The GPS jamming threat units embody the University of Bath and Chronos Technology algorithms described in Section 4.2 above. They communicate with the server via the host's network, either as a VPN or via a 3G or 4G communications link. In the latter case the sensor is mounted in a rapidly-deployable weatherproof enclosure with a UPS and a remote re-booting facility.

Key features of both devices are summarised below.

8.2.1 THE SENTINEL SENSORS

The Sensor is housed in a 19" 1U rack mount unit. There are a number of versions, as outlined in the Table below.

Figure 35: GAARDIAN/SENTINEL Sensor

Table 1: Sensor types

Sensor Version	Feature	Description
Version A	UoB Algorithm	"QuickThresh" Algorithm developed by UoB*
Version B	UoB and FFT1 Algorithm	Adds FFT Algorithm
Version C	UoB and FFT2 Algorithm	Replaces FFT1 with FFT2 Algorithm on new Hardware

Version C sensors were designed with a faster FFT feature (FFT2) to enable real-time geo-location of jamming and are available with the Signal Sentry™ 1000 system from Exelis.

The SENTINEL network comprises sensors in Versions A and B. Transition from Version A to B or Version A/B to C would require a hardware upgrade within the sensor.

8.2.2 SENTINEL SERVER OPTIONS

Two Server options are available.

Version A is the SENTINEL Research Platform which has been fully operational for approximately 3 years. Some sensors have been in continuous operational since early 2011. It has unlimited scalability regarding the number of sensors and allows multiple simultaneous network operations. This version is compatible with Sensor Versions A and B.

This version is in use with multiple clients for demonstration purposes where it illustrates the nature and extent of any jamming threat.

Version B has the capability to geo-locate the source of the jammer in a finite mesh of Version C Sensors.

Table 2: Server Types

Server Version	Feature	Description
Version A	SENTINEL Research Platform	Hosted by Chronos.
Version B	Geo-location Features	Signal Sentry™ 1000 System

8.2.3 SENTINEL RESEARCH AND DEMONSTRATION SERVER GUI FEATURES

The Server is hosted in the Cloud. It can be reached via a 'unique' URL, using a Username and Password. A server can be configured with Viewer, Manager, Expert and Administrator rights. It is available either as a basic research platform or for demonstration purposes.

A feature set is summarised below

Table 3: Server Features

Feature	Description
Default GUI Display	SatCat Logo, OS Opendata
Optional GUI Displays	Google, OpenStreetMaps, CloudMade, BlueMarble
Sensor Details	Status and Location
GPS Status	Time, date, PDOP, HDOP, VDOP, Tacc
GPS Satellite Data	PRN, Elevation, Azimuth, SNR, Polar Display
UoB "QuickThresh" Events	Event List: Start Time, Duration, Satellites affected, filtered by duration
UoB "QuickThresh" Analysis	Event Analysis by: Month, Day, Hour during Day, Day of Week
FFT Events	Event List: Start Time, Duration, Satellites affected, filtered by duration
FFT Analysis	Event Analysis by: Month, Day, Hour during Day, Day of Week
Change Password	Ability to change password
Alert Subscriptions	Ability to receive email event alerts

8.2.4 EXELIS SIGNAL SENTRY™ 1000 SYSTEM

Exelis (Formerly ITT Geolocation Systems) approached Chronos Technology in 2011 to explore collaboration in a development project. The object was to deliver a service to report on the signal quality of GPS in a location where it was to be used by mission-critical or safety-critical services. Exelis have significant experience of GPS technology, since they supply the GPS Block III satellites' payload electronics and the new ground-segment monitoring capability OCX.

The solution that emerged from the collaboration was an enhanced sensor designed and supplied by Chronos Technology. It delivers data to an Exelis server which incorporates a geo-location algorithm. This has enabled real-time geo-location of a jammer when tested in Sweden (see Section 10.3 below). It is now operational in a number of trial networks.

"GPS is used to control and track business in real time. Signal Sentry™ 1000 protects assets and keeps commerce churning. Signal Sentry™ 1000 has the unique capability to simultaneously locate up to 3 disruptive sources utilising a proprietary algorithm (patent pending). It supports today's mobile organization with a user interface built upon standard protocols; a user can securely log into the system from any web enables decide – including tablets and smart phones – providing actionable intelligence at the point of need." Exelis Inc.

"Signal Sentry™ 1000 leverages signal domain knowledge of the Global Navigation Satellite System. Exelis is the leading global provider of PNT products, systems and solutions with over 40 years of demonstrated performance for military, civil, government and commercial customers depending on reliable and secure GPS navigation and timing services. Exelis has provided payloads to 113 GPS satellite missions. There have been no failures due to Exelis hardware or software with over 500 years of cumulative on-orbit operations. Simply put, Exelis is the assured GPS provider." Exelis Inc.

"A Clear Reality: Exelis worked with UK-based Chronos Technology on this solution. Chronos applied their learning from the GAARDIAN and SENTINEL research programs, partly funded by the Technology Strategy Board – the UK's innovation agency supporting business-led innovation. These programs helped quantify the clear and present threat of GPs jamming; Signal Sentry™ 1000 leverages the sensor technology that emerged from the research." Exelis Inc.

8.3 SENTINEL AS A 24X7 PNT RESEARCH PLATFORM

The use of the SENTINEL platform, both server and sensors, for research related to Resilient PNT has continued long after the ending of the original task of exploring the threat of GPS jammers. These later projects comprise a mixture of self-funded research by Chronos Technology and responses to requests from third-party organisations. They include many varied research and demonstration requirements including the field analysis of GNSS technology, jamming or interference phenomena and timescale transfer projects.

The flexibility of the server architecture allows private jamming-detector networks to be set up which share a central server in the Cloud. Alternatively, an individual server can be hosted within a client's own secure environment or even field-deployed for remote work, being recovered at the end of a trial. In this way, 24x7 testing can be enabled with configurable data-reduction and analysis techniques.

Activities which either have been, or could be, undertaken include:

- eLoran Research – see Section 8.3.1
- Vulnerability mitigation techniques - see Section 8.3.2
- GNSS application vulnerability analysis – see Section 8.3.3
- Spoofing research
- Antenna testing
- Other non-GPS GNSS performance analysis
- UTC time scale delivery and comparison
- Field jamming and interference monitoring
- Algorithm development
- Data Analysis development
- Student GNSS vulnerability and mitigation tutorial and demonstration facilities

8.3.1 ELORAN: CTL8200 - THE ELORAN PROOF-OF-CONCEPT UNIT

SENTINEL successfully showed that eLoran$_{UTC}$ is comparable in quality to GPS$_{UTC}$ and so can be a candidate as a viable solution when GPS vulnerability is to be mitigated.

In order to explore this possibility further, a Proof-of-Concept eLoran timing receiver (CTL8200) has been created from the SENTINEL Sensor. The CTL8200 is a timing receiver with inputs from GPS and eLoran. The user can evaluate UTC taken simultaneously from GPS satellites and selected eLoran stations continuously in real-time.

Figure 36: CTL8200 eLoran Timing Receiver

The receiver is an enhanced development based on the earlier units employed in the GAARDIAN and SENTINEL projects. It embodies the latest eLoran receiver technology from UrsaNav Inc. All this is incorporated within a single 1U 19" chassis.

There is strong complementarity between eLoran and GPS. For example, the CTL8200 automatically calibrates the fixed delay in the eLoran$_{UTC}$ by reference to the GPS$_{UTC}$ when it is first installed at a site. Thereafter, it outputs a UTC-aligned 1pps that is independent of GPS and immune to any disruption of GPS by interference, jamming or spoofing of the GPS signal. Moreover, since the eLoran signal is inherently resilient to the failure or downtime of any individual eLoran station, the eLoran$_{UTC}$ can be used to indicate that GPS$_{UTC}$ is being spoofed.

A full datasheet on the CTL8200 can be found here.

8.3.2 VULNERABILITY MITIGATION TECHNIQUES – CRPA TECHNOLOGY

Figure 37: CRPA Antenna

Controlled Radiation Pattern Antenna (CPRA) technology is emerging onto the civil market from its military origins. Whilst for military use it is regarded as being at Technology Readiness Level 1 (TRL1), the Size Weight and Power (SWaP) quotient and the cost are both too high for industrial use; in that context it must be considered as being at TRL5 or 6.

Recent SENTINEL trials of CRPA technology in an electrically-noisy location have shown its promise as a way of reducing the impact of local jamming and radio frequency interference (RFI) on either a SENTINEL sensor or a GPS receiver. Further information regarding these tests may be had by contacting charles.curry@chronos.co.uk.

8.3.3 GPS APPLICATIONS – ANALYSIS OF VULNERABILITY

Aircraft instrument landing systems that use GPS have been under development for a number of years. Those technologies that employ augmentations systems receive either GBAS signals or SBAS using EGNOS, WAAS or MSAS according to region (see APPENDIX E for definitions of these terms). These augmentation systems monitor and report on the GPS signals, so assuring integrity and enhancing accuracy.

There is concern that GPS jamming will disrupt such landing systems, reducing availability and continuity (APPENDIX C). Aeronautical agencies in a number of countries have expressed interest in deploying the SENTINEL research platform to investigate the nature and extent of this threat.

9 DISSEMINATION OF INFORMATION

A key eligibility requirement for TSB collaborative R&D funding is a viable exploitation strategy for products and services; this becomes quite a challenge when no market exists and most potential users are not even aware of the potential threat! In that situation, one must use publicity to educate them.

SENTINEL (and GAARDIAN before it) set out to bring the GPS vulnerability threat to the attention of organisations responsible for mission-critical and safety-critical applications of GPS. They did so through press articles and interviews, plus papers and presentations at symposia and conferences.

Both the SENTINEL and the earlier GAARDIAN projects received wide coverage in the national, international and trade press. The SENTINEL project has been so widely presented that it was showcased at symposia in 5 different countries over a single 7-day period during April 2013, demonstrating the global importance of the work. Preparing and delivering these presentations has required great care to ensure that professional information was disseminated without either scaremongering or excessive promotion of products!

9.1 PRESS ACTIVITY

The appetite of the trade press for information on activity relating to SENTINEL and GPS jamming has been quite extraordinary. The ability of many professional journalists to listen, comprehend and report on the project in a measured way without hyperbole, given the threats it has disclosed, has been most rewarding. There have been feature articles in the Guardian, the Daily Telegraph, The Economist, and The Independent plus coverage on BBC News. The Economist feature headlined "Out of Sight"[12] is an example of a piece of good reporting that reviews the importance of satellite positioning capability and explains the ease with which it can be disrupted. See APPENDIX A for a list of some of the links to press stories. Just entering "SENTINEL GPS Jamming" into a search engine will bring up many hits.

9.2 SYMPOSIA & CONFERENCE PRESENTATIONS

Papers and PowerPoint presentations delivered at many symposia and conferences around the world have delivered a significant global benefit in terms of spreading the message about GPS jamming and opening up further collaboration and exploitation opportunities. Indeed the links with the US organisation Exelis resulted from a Web search by one of their technology capture staff which turned up a presentation delivered in 2011 at the KTN-sponsored PNT event on GPS jamming held at NPL. This symposium, the first in what is now a regular annual series co-sponsored by the Royal Institute of Navigation, was proposed to the KTN by SENTINEL participants.

See APPENDIX D for a list of Symposia and Conference Presentations.

9.3 FEATURE ARTICLES

Feature articles have appeared in Inside GNSS
http://www.insidegnss.com/auto/sepoct11-Proctor.pdf

and the Society of Motor Manufacturers & Traders Research Newsletter
http://smmtacuknewsletters.cmail2.com/t/ViewEmail/r/5207D728374733612540EF23F30FEDED/45D182B3400974361726EA5DA1051479

Bloomberg TV featured the GPS jamming incident which affected Newark Airport
http://www.bloomberg.com/video/88574724-gps-jammers-threaten-air-traffic-navigation.html

Commercial Motor featured the article Concern grows over GPS jammers on 6 Dec 2013
http://www.commercialmotor.com/latest-news/concern-grows-over-gps-jammers

The Economist wrote: Satellite positioning data are vital – but the signal is surprisingly easy to disrupt

[12] The Economist article can be found on this link Out of Sight

http://www.economist.com/news/international/21582288-satellite-positioning-data-are-vitalbut-signal-surprisingly-easy-disrupt-out

SouthWestBusiness reported: Gloucestershire firm's technology helps in the fight against satellite jamming http://www.southwestbusiness.co.uk/news/05022013082459-gloucestershire-firm-s-technology-helps-in-the-fight-against-satellite-jamming/

10 GPS JAMMING TRIALS

A number of GPS jamming trials have taken place both during and after the formal research project. These were conducted at three locations: at Sennybridge in the Brecon Beacons; at The Motor Industry Research Association (MIRA) centre at Nuneaton; and in Sweden, by permission of the Swedish Defence Research Agency. The tests helped greatly in assessing the effective ranges of the various GPS jammers and in establishing the ranges over which they could be detected.

10.1 UK TRIALS – SENNYBRIDGE

The UK trials on the Sennybridge military range were the first UK trials conducted by a non-military consortium using civilian jammers. Three sessions took place: in June 2011, June 2012 and October 2012. The weather was not always predictable and the trials teams had to contend with sun, hail and horizontal rain.

In order that the Sennybridge trials could be conducted legally, they had to be managed by the Ministry of Defence (MoD) and announced well ahead of time by OFCOM. OFCOM were informed in advance of the powers, frequencies and times of transmissions. They then issued a notification of the trial through its web site and via email.

Among the jammers tested were some that had been seized by OFCOM and the one seized by an LEA in the course of the SENTINEL project (see Section 6 above). Lessons learned during these trials helped in optimising the design of the jamming detection equipment.

The jammers themselves had to be modified to disable all non-GPS jamming signals. A most significant discovery was that the effective ranges of most of the low-powered jammers greatly exceeded their advertised ranges: one with a claimed range of a few metres had a measurable impact on receivers over a 250m radius. Jammers like this can significantly and dangerously threaten critical infrastructure that relies on GPS signals.

Some trials included driving vehicles containing jammers at speeds of up to 70 mph to test the effectiveness of the detection equipment and its ability to discriminate actual jamming from general interference and its ability to identify which vehicle contains a jammer.

OFCOM publish jamming notices on this web link
http://stakeholders.ofcom.org.uk/spectrum/gps-jamming-exercises/

10.2 UK TRIALS – MIRA

Figure 38: Vehicles in MIRA Test Facility

The trials at MIRA were conducted in a large screened room facility. They were of particular value in allowing the direction-finding features of the CTL3520 hand-held detection unit to be tested. Three cars were driven into the largest screened room facility - Figure 38. A jammer had been placed in the boot of one of the cars. Representatives of LEA and security agencies witnessed as the car was identified and the jammer recovered. The purpose of the trial was to demonstrate the direction-finding capability of the CTL3520 hand-held jammer detector. Tests were 100% successful: the CTL3520 was able to locate a jammer on a specific floor of a building and in the pocket of an individual.

10.3 SWEDISH TRIALS – SWEDISH MINISTRY OF DEFENCE - FOI

Figure 39: Field Deployed Sensor in Weatherproof enclosure

GPS Jamming Trials were conducted on a military test range north of the Arctic Circle in Sweden in early September 2013. The tests, in which Exelis collaborated, were held under the auspices of FOI, one of Europe's leading research institutes in the areas of defence and security. FOI's core activities are research, methodology/technology development, analyses and studies. FOI is an assignment-based authority operating under the Swedish Ministry of Defence.

The purposes of the trials were to field-test the Exelis Signal Sentry™ 1000 geo-location capability which uses the enhanced SENTINEL sensor and also to test further the direction-finding capability of the CTL3520.

Figure 40: CTL3520 in use

The picture on the left shows one of the field-deployed sensors on a tripod with its wireless communications; that on the right shows the CTL3520. They were locating a jammer hidden in the long grass. An array of sensors communicating via wireless links with a field-based server successfully geo-located jammers in real-time with an accuracy of approximately 10m.

11 CONCLUSIONS

Since GAARDIAN began in 2008 the phenomenon of GPS jamming has been ever-increasing. The SENTINEL Project has become a catalyst for cross-border collaboration between law enforcement agencies and security services, as they have explored this threat. The data produced has resulted in a much better understanding of the problem within organisations responsible for critical national infrastructure and homeland security.

SENTINEL continues to demonstrate that jamming is getting worse: some probes are now detecting 5 to 10 events per day; over 50 web sites are actively selling jammers; and the devices being seized by law enforcement agencies are now more powerful and so have considerably greater jamming ranges. Whereas in 2008 GPS was the only satellite PNT system under threat, and jamming targeted its L1 frequency alone, now all frequencies of all GNSS are under attack. This includes both the Open and PRS services of Galileo.

Thanks to SENTINEL, GNSS vulnerability is now widely reported and much better understood by professionals and, to a lesser degree, by the public and policymakers.

Mitigation options are emerging: these range from "sticking plaster" solutions to a complete alternative PNT technology. The furthest-developed alternative is Enhanced Loran (eLoran). Helped by SENTINEL, its low-frequency signals have now reached limited Initial Operational Capability for shipping and precise timing in the UK and Ireland. There are firm plans to install eLoran in South Korea and the technology is being considered for strategic deployment in Saudi Arabia, India and other countries. Europe and the USA urgently need to study the impact that a Black Swan event like the one North Korea afflicted on South Korea would have, and commit to a long-term investment in sustainable and resilient PNT for many areas of strategic infrastructure. Whilst eLoran can serve multiple applications, the specialised roles of other technologies, as set out in this Report, should also be studied. The argument that alternative GNSS solutions such as Galileo can mitigate these multi-frequency threats to strategic fixed infrastructure is no longer viable.

It is now 36 years since the first Block 1 GPS satellite was launched and nearly 20 years since major telecoms networks started to contemplate using GPS timing. A trans-national commitment to eLoran for a minimum 20-year period would secure reliable and resilient PNT in the long term.

12 AKNOWLEDGEMENTS

A project of this scope and scale cannot be undertaken by a single organisation. Many companies and individuals have provided invaluable contributions to SENTINEL. Between them, they have developed ideas and theories, conducted debates, and advised on project management. The result has been a project that has been recognised around the World as technologically innovative; it has pushed the boundaries of knowledge and delivered a significant socio/economic dividend.

In particular, thanks go to:

The Association of Chief Police Officers – Intelligent Transport Systems (ACPO-ITS) – Chief Superintendent Jim Hammond and his team for enabling jamming trials, hosting locations and providing insight into the ways of working of Law Enforcement Agencies (LEAs).

Chatham House – David Clemente for recognising the significance of the threat and inviting presentations at two Cyber Security events.

The General Lighthouse Authorities of the United Kingdom and Ireland (GLAs) – Dr Sally Basker for her early enthusiasm when forming the GAARDIAN consortium; George Shaw for his solid support and dedication to the team; Dr Paul Williams for his superior knowledge on all things about eLoran; Martin Bransby for his dedication to the project; and Chris Hargreaves for his work on the eLoran QoS algorithm.

National Air Traffic Services (NATS) – Ken Ashton for facilitating the placing of a SENTINEL sensor close to the runway of a busy airport.

National Physical Laboratory (NPL) – Bob Cockshott for diligently walking the streets of London with a detector in his pocket and scoring more hits than anyone else; also for steering the Knowledge Transfer Network (KTN) to its focus on the GNSS Vulnerabilities series of symposia; David Hindley for coordinating the NPL team and being at every meeting; Dr. Peter Whibberley & Dr. John Davies for their assistance in calibrating timing systems to UTC and their work in monitoring $eLoran_{UTC}$ (with apologies to John for causing the only outage in 3 years of data!)

OFCOM – Clive Corrie and Steve Harding for making available GPS jammers they had seized and for sage advice on the testing of jammers.

The Ordnance Survey (OS) – Dr. Mark Greaves for arranging for OS Net sites to become host locations for SENTINEL and for informed and regular debates while analysing events in order to assess their authenticity.

The University of Bath (UoB) – Prof Cathryn Mitchell for her wise words and knowledge of GPS anomalies, Space Weather and in particular for developing the "QuickThresh" algorithm which became the key to

jamming event detection; Dr Jenna Tong for her work on the QuickThresh algorithm and data analysis; Dr Robert Watson for his deep knowledge and pragmatic contributions throughout the project and in particular for his work on hand-held jammer detectors; and Dr Nathan Dumont for turning Dr Watson's ideas into reality.

The Technology Strategy Board (TSB) – Andrew Tyrer and Tim Just for their belief in the project and their support during the work and afterwards; Alan Bennett who as monitoring officer showed considerable patience with the team and offered wise and constructive advice on reporting and other TSB administrative requirements.

Thatcham Vehicle Security (TVS) – Martyn Randle for advice on vehicle security systems.

Prof. David Last - for his wise guidance on many topics relating to eLoran transmissions and technology, GNSS vulnerabilities and, in particular, proof-reading and amending this report.

Members of various UK and US Security and Government departments, who shared and reviewed SENTINEL data but who, by virtue of the nature of their roles, must remain anonymous.

Last but not least many staff at Chronos, the SENTINEL lead partner, not named individually but who guided the project technically and administratively, built the Web server, translated Matlab to C++ running under Linux, overcame bureaucratic hurdles to the installation of sensors, ran trials in challenging locations and environments and met deadlines in delivering products.

13 REFERENCES

a) Royal Academy of Engineering – Report on GNSS Vulnerabilities.
b) Society of Motor Manufacturers and Traders – Summer 2013 Research Newsletter
c) Dependency of Communications Systems on PNT Technology – Charles Curry, March 2010
d) GPS Antenna Installations. Best Practice – Chronos Application Note
e) UK Government Office for Science Report "The Future of Computer Trading in Financial Markets"
f) "Protecting the UK Infrastructure: A System to Detect GNSS Jamming and Interference" – SENTINEL White Paper

APPENDIX A EXAMPLES OF PRESS COVERAGE

A.1

22 Feb 2012 - "The idea behind *Sentinel* is to detect and locate interference," *Chronos* told ZDNet UK on **...**

A.2

10 Dec 2010 - *Chronos* Technology is leading a consortium, *SENTINEL*, which is a 24 month project to research and develop a service to establish the extent **...**

A.3

21 Dec 2010 - *SENTINEL* keeps an eye on GPS. 21 Dec 2010. UK Company *Chronos* Technology is leading a consortium developing a system that monitors **...**

A.4

Chronos will be demonstrating the *Chronos SENTINEL* system which enables a light touch deployment of GPS jamming detection for a short period of time and **...**

A.5

13 Sep 2013 - Exhibiting at Stand 723, Chronos will be demonstrating the *Chronos Sentinel* system, which enables a light-touch deployment of GPS jamming **...**

A.6

SENTINEL project research reveals UK GPS jammer use
21 Feb 2012 - In one location the *Sentinel* study recorded more than 60 GPS jamming **...** of *Chronos* Technology, the company leading the SENTINEL project …

A.7

*news.sciencecitybristol.com/nowhere-to-hide-**chronos**-technology-detect...*
13 Jun 2012 - *Chronos* is the UK leader in time and timing for fixed and mobile telecoms, **...** "With *SENTINEL* we set out to do more than just detect: we are **...**

A.8

FIVE, Farnborough, 12 March 2013, *Chronos* Technology demonstrates SENTINEL to James Brokenshire, Minister for Security

A.9 

Charles Curry delivers presentation at NIST WSTS – GNSS Jamming – Quantifying the Threat

A.10 

Protecting the UK infrastructure *SENTINEL* – A system to detect GNSS Jamming and Interference

A.11 

17 July 2013 *Chronos* Technology, a global **...** and is a significant commercial outcome of the *SENTINEL* research project **...**

A.12 

GAARDIAN, a collaboration led by *Chronos* Technology Ltd., included the University of Bath **...** a concept being used in the successor program, SENTINEL

A.13 

14 Dec 2010 - Specialist electronics firm *Chronos* Technology is the lead partner in Sentinel, research projecting aiming to tackle GPs jamming that can disrupt police operations and interference with airport navigation systems

A.14 

18 Nov 2011 - Rochester NY (SPX) Nov 18, 2011 - ITT Exelis and *Chronos* **...** the lead for the UK Government sponsored SENTINEL research program,

A.15 

22 Feb 2012 – GPS jammer usage increasing in UK reveals Sentinel project **...**

A.16 

23 Feb 2012 – Research by the Government-backed Sentinel consortium shows dangerous GPs jammer use in the UK is on the rise.

There is an excellent comment sequence after this story including:

"People use jammers because of companies like mine..
they recently installed GPS black boxes in all our vans, and have set them to report back ALL and ANY speeding incidents, it even reports back if you are doing 31 in a 30, 41 in a 40 etc, and the company then invite you for 'informal' chats about your speeding and complacent attitude to safety… they have started a 100% zero tolerance policy against speeding…
I am thinking of getting one myself now I have read this article…"

And:

"….You've failed to consider people like myself – regular commuters who are fed up with inconsiderate selfish idiots who insist on having phone conversations at full volume on a packed train at rush hour, even in a quiet carriage.

Having done this every day for years, I was fed up with conversations consisting of "yeah yeah, innit, like, cos innit"…etc; if you try and ask them to be quiet you typically get a mouthful of abuse; this is a far less confrontational, and yet satisfying way to resolve the problem…."

A.17

17 Nov 2011 - ITT Exelis (NYSE: XLS) and *Chronos* Technology Ltd. Team to develop offerings for the Interference, Detection and Mitigation Market… SENTINEL research program, **...**

A.18

24 Feb 2012 - Set up by the government's Technology Strategy Board (TSB) and run by *Chronos* Technology UK, the Sentinel network **...**

A.19

13 Feb 2013 - **...** Moonlighting van drivers are probably to blame for the growing problem of GPS jamming on Britain's roads, the latest survey of the problem by the Technology Strategy Board's SENTINEL project has suggested.

A.20

15 Apr 2011 – GPS vulnerability to hacking

A.21

22 Feb 2012 – GPS jamming: a clear and present reality - Set up by the government's Technology Strategy Board and run by *Chronos* Technology, the Sentinel network **...**

A.22

ITT Exelis is excited to collaborate with *Chronos* Technology to address this **...** UK Government sponsored SENTINEL research program, which followed on from **...**

A.23

10 Mar 2011 – Navigation: as the uses of satellite-positioning technology continue to grow, what can be done to stop deliberate and dangerous jamming of the signals….. That is where SENTINEL comes in.

A.24

22 Feb 2012 - The Sentinel project is a collaboration between *Chronos* Technology, which provides the interference-detecting probes, and the ICT **...**

A.25

17 Nov 2011 - ITT Exelis and *Chronos* Technology Team to develop offerings for the **...** the UK Government sponsored SENTINEL research program, which **...**

A.26

Chronos Technology, last month released a handheld GPS jamming detector and **...** of the SENTINEL research project which was part-funded by the Technology **...**

A.27 

... Global Navigation Satellite System technology (e.g., GAARDIAN, SENTINEL). Current industrial research collaborators include *Chronos* Technology,

A.28 

17, 2011 – ITT Exelis and Chronos Technology Ltd. have **...** the UK Government sponsored *SENTINEL* research program, which followed on from **...**

A.29 

A rise in the number of cases of GPS jammers poses a serious threat to fleets. Research from the SENTINEL consortium reveals

A.30 

The UK 'relying too heavily' on Sat Navs

A.31 

Thousands of people are using GPS jammers to disguise the fact that they are driving stolen cars, or to hide the fact that they are driving commercial vehicles for dangerously long hours……

A.32 

Thousands using GPS jammers on UK roads pose risks, say experts …

A.33 

Car Thieves using GPS jammers – jammers overwhelm anti-theft devices on cars and lorries .. later versions could be used to disrupt air traffic

A.34 

Organised crime routinely jamming GPS

A.35 

Satellite positioning data are vital – but the signal is surprisingly easy to disrupt

A.36 

A blog on a jammer web site which mentions SENTINEL and (rather amusingly!) refers to the findings as "lies, lies and again – lies!"

A.37 

TomTom believes better education for drivers on the benefits of vehicle tracking systems may reduce the use of GPS jammers on Britain's roads.

A.38

13 Sept 2013 – Exhibiting at Stand 723, Chronos will be demonstrating the Chronos SENTINEL system which enables a light-touch deployment of GPS Jamming

A.39

9 January 2014 - A Melbourne taxi driver was recently convicted and fined $850 by the Magistrates Court for recklessly engaging in conduct that would cause substantial interference to Radiocommunications (section 197 of the *Radiocommunications Act 1992*).

The prosecution was the result of a joint operation between the Australian Communications and Media Authority and the Victorian Taxi Services Commission to combat GPS jammer use within the Melbourne taxi industry. The driver, who pleaded guilty, was detected operating a GPS jammer in the CBD through ACMA surveillance techniques.

A.40

9 January 2014 – Melbourne cabbie fined over GPS jammer – Radio comms could be blocked in fight for passengers

A.41

Jan/Feb 2014 – SENTINEL Solutions now available from Chronos Technology

APPENDIX B ON-LINE AVAILABILITY OF GPS JAMMING DEVICES

B.1 JAMMER SITE BLOGS

There are many web sites available selling jammers. Some are listed below. Their claims make interesting reading…

There is an excellent blog page on the web site www.jammer-store.com about SENTINEL and the GP5000, written perhaps by a disgruntled non-technical sales support person.

Entitled "Chronos Sentinel Project: Many Lies About GPS Jammers" published in March 2012 this Report picks up the blog half way through….

"But let us continue the story. Sentinel Project used 20 roadside monitors for GPS jammer detection. They have been catching all cars with GPS jammers inside passed by those sensors. And they have determined that there are approximately 50-450 cases of GPS jammer usage in UK cars every single day. Nice job guys! But there it comes, the thing that I will cite because it is probably the biggest lie in the whole article:
"He told the BBC that evidence from the project suggested that most jammers were small portable devices with an area of effect of between 200m and 300m."

Lies, lies and again – lies!

Small portable GPS jammers physically cannot have effective jamming radius of 200-300 meters! Just look at these GPS jammers: GP5000 used in cars, GJ6 portable GPS jammer and RCJ40-D adjustable desktop jammer. Even the most powerful desktop model that I can hardly imagine working in someone's car (it has no car power adapter) has the jamming radius of 40(!) meters but not those 200-300 which were said about in the BBC News article."

Apart from the technical inaccuracies and mis-reporting of the facts behind the SENTINEL network, it is flattering to think that information relating to the SENTINEL Project has found its way to China.

One web site advertises the J-242 model with the benefits "Does (sic) your company car equipped with a GPS system and you are monitored by your boss? Do you suspect your jealous partner (sic) having you watched or monitored? Now, You have The chance of being Undisturbed and Untraceable!"

The Manufacturer – WolvesFleet helpfully provides the following advice "It can be applied at meeting room, conference room, museum, gallery, theatre, concert hall, church, temple, restaurant, classroom, training centre, factory, bank, train, bus, etc. For some locations of special purpose such as hospital, gas station, etc., please do field test first to make sure no interference happened to the normal operation of their equipment and instrument. It is easy to install and operate the device."

B.2 JAMMER4UK.COM

http://www.jammer4uk.com/

Comments on this web site include:

"Being an ISO 9000 / 9001 / 9004 / 19011: 2000 certified organization, established by Shenzhen Government at 1993, we offer a voluminous range of premium quality jammer products from multi band, very high power jamming systems, Vehicular Jamming system, Multi band Jamming system, Indoor and Outdoor Jammers (Cellphone Jammers, GPS Jammers, Wireless camera Jammers), for the protection of troop transportation, Military and Police checkpoints, large Governmental establishments, Bomb Disposal Squads and VIP convoys."

"We will write "Signal Booster" or "signal receiver" or "RF ROUTER" on the package, also describe the contents value as $10 each and describe it as a "GIFT", this way it will avoid being caught by Customs for Import taxes!"

B.3 WWW.JAMMERFROMCHINA.COM

http://www.jammerfromchina.com/categories/GPS_Jammers/

Comments on this web site include:

"And there are different types of GPS signal jammer, as GPS jamming devices are portable or desktop style devices that can work to stop a GPS tracking device from receiving the signal and by using GPS jammers the operator of the GPS tracking device can't pick up their position. GPS signal jammers can emit their own signal at the frequency that GPS tracking devices use, which confuses or blocks other GPS signals.

When choosing the GPS signal jammers, you need to make clear which frequency bands of GPS signal that you want to cut off, and then you can choose and pick up the right one. And as there are handheld, mini, desktop, and high power GPS jammer for sale, or the ones that only designed for car using. It is also necessary for you to choose one that can meet your details take the above factors into account."

B.4 WWW.DHGATE.COM

http://www.dhgate.com/wholesale/gps+jammers.html

B.5 WWW.GLUSHILKA.COM

http://glushilka.com.ua/glushilka-gps-gsm.html

This web site, based in the Ukraine, is the first European site to be found openly selling GPS jammers.

B.6 WWW.ALIEXPRESS.COM

http://www.aliexpress.com/w/wholesale-gps-jammer.html

Comments from this web site:

*"We know you're passionate about your vehicle - that's why we're driven to provide you with everything you need to keep your car, motorcycle or ATV running and in top condition. At AliExpress.com, you can browse **wholesale gps jammer**, wholesale car parts, wholesale automotive accessories and equipment for motorcycles from **Chinese gps jammer wholesalers**. We also have a great selection of cheap anti tracker, cheap gps detector, cheap gsm gps.*

So variety isn't a problem. But what about price? We all know that routine maintenance can extend the life of your vehicle by years, but all those tools cost money. That's why we offer anti tracker promotion, gps detector promotion, gsm gps promotion from numerous gps jammer wholesalers! You can find all the wholesale information you need - from anti tracker reviews, gps detector reviews, gsm gps reviews and gps finder price, wifi jammer price, radio jammer price. So whether you're looking for an oil change or a new air filter, let AliExpress.com be your co-pilot."

B.7 WWW.CHINAECARTS.COM

http://www.chinaecarts.com/gps-jammers-c-42_44.html

Comments from this web site include:

"Congratulations, You Have Found the Internet's Best Source of Buy Wholesale GPS Jammers! Check Out Chinaecarts's Online Shop, You Will Find an Awesome Array of Buy Wholesale GPS Jammers - GPS Jamming."

B.8 WWW.ALLJAMMER.COM

http://www.alljammer.com/portable-gps-jammer-gpsl1l2-p-147.htm/

B.9 WWW.CHINAJAMMER.COM

http://www.chinajammer.com/

B.10 WWW.ALIBABA.COM

http://www.alibaba.com/showroom/gps-jammer.html

B.11 WWW.CHINAVASION.COM

http://www.chinavasion.com/china/wholesale/Security_Equipment/Jammers/Covert_Portable_GPS_Jammer

Comments from this web site include:

"Covert Portable GPS Jammer - Are you sick of being tracked like a criminal? This portable GPS jammer will ensure you can do what you want without big brother looking over your shoulder. Lightweight and easy to conceal this jammer will block all GPS traffic out to a range of 10m from the device. Useful car and mains power adapters are included to ensure protection all day. Great for use in the company car for when you choose to have a long lunch.

Buy now from Chinavasion at our factory direct wholesale price with factory direct low china wholesale price and we'll even dropship it to your customer. Better still, get one for yourself and then buy additional units to resell on eBay to other concerned citizens. Make money for yourself and also help people protect their privacy - a win-win for everyone! Get yours now!!"

B.12 WWW.JAMMER-STORE.COM

http://www.jammer-store.com/gps-blockers-jammers.html

Comments from this web site include:

"As you may already know, location tracking these days might be not only helpful but also it can violate your privacy rights because many law enforcement agencies in different countries practice warrantless tracking. They place tracking devices under your vehicle and monitor your location at will because privacy laws are incomplete in those countries. To help you manage this situation there are GPS jammers to be used. Those devices can prevent satellite tracking systems of any country from finding out where you are."

B.13 WWW.JAMMERALL.COM

http://www.jammerall.com/news/214/Best-Buy-a-GPS-Signal-Jammer-with-a-Reasonable-Price.html

Comments from this web site include:

"Ruin every single plan of being tracked by those bad men, how to do to achieve this goal, best buy a high power GPS jammer with a reasonable price, you can get one from www.jammerall.com. When you get the first chance to know something about the name of GPS signal jammer, how do you think? About its function and design what to you exactly? Maybe it is after a period of learning and knowing, you will know that the device is specially designed for disabling the GPS tracking system from getting the accurate positioning.

Started from 1973, the GPS devices were used by the United States for finishing the secret tasks in the military missions as a helping weapon to find out the right position for explosion and defeat. At that time, the history of the GPS devices had been written firstly as a horrible weapon. With time goes on, it has been changed slowly for more usages in our daily life, some of them are helpful, while some of them are really terrible for our routine life normal going on. So next will be the show time of our today's hero- GPS signal jammer."

B.14 WWW.MADE-IN-CHINA.COM

http://www.made-in-china.com/products-search/hot-china-products/Gps_Jammer.html

B.15 WWW.ESIONWILL.COM

http://www.esionwill.com/index.php?main_page=index&cPath=782&productsort=3

B.16 WWW.SECURITYGADGET.ORG

http://www.securitygadget.org/portable-handheld-cell-phone-wifi-gps-signal-jammer-up-to-8-meters.html

Comments from this web site include:

"Most people want to enjoy the peaceful life and just don't want disturb by others after work or in weekends. In this situation this Handheld Cell Phone & WiFi & GPS Jammer can be a good choice."

B.17 WWW.THEFIND.COM

http://www.thefind.com/electronics/browse-portable-gps-jammer

B.18 WWW.CHINAJIAHO.COM

http://www.chinajiaho.com/high-power-signal-jammer-for-gps-cell-phone-3g_p2579.html

B.19 WWW.JAMMERFUN.COM

http://jammerfun.com/gps-jammer.html

Comments from this web site include:

"GPS Jammer : Welcome to your one-stop wholesale GPS Jammer shop, In here, you will find the best car gps jammer, gps signal jammer, gps gsm signal jammer, gps jammer blocker, jammers dropship, jamming device wholesale with lowest price and high top quality direct from China jammers manufacturer. Jammerfun has what you are looking for, and has a wide range of the best anti-surveillance and anti-mobile phone security."

B.20 WWW.PAKBIZ.COM

http://pakbiz.com/profile/Shenzhen-Jinyatong-Techonology-Co-Ltd/Mini-Portable-Cell-Phone-GPS-Jammer_PID22057.html

Comments from this web site include:

"If you are sick of all those phones going off, or being tracked everywhere with GPS, this is the anti-spy gadget you have been looking for. This jammer system comes with a built in rechargeable Li-ion battery for hours of signal jamming, and with the included car power adapter, recharge and use this in your car as well as the office. Incredible easy to operate, just switch it on and it will immediately start blocking any GPS tracking device signals will keep noise and other disturbances away."

B.21 WWW.CELL-JAMMERS.COM

http://www.cell-jammers.com/gps-jammers.html

Comments from this web site include:

*"This **CAR GPS JAMMER** is a popular item with sales personnel and delivery drivers, who wish to take lunch or make a personal stop outside of their territory or route "off the radar". Simple to use, just plug into a standard cigarette lighter with 12V for power, and the GPS Jammer will automatically protect you by blocking any GPS tracking on and within your vehicle."*

APPENDIX C NEWS STORIES AND VIDEO PRESENTATIONS REGARDING GPS JAMMING

These video and radio broadcast links have been collected during and after the SENTINEL project.

C.1 BBC RADIO 4 – QUENTIN COOPER: FINDING A WAY: THE FUTURE OF NAVIGATION - 2013

http://www.bbc.co.uk/programmes/b038yq98

Prof. David Last, Prof. Cathryn Mitchel, Prof. Charles Curry and Dr. Paul Williams were interviewed by Quentin Cooper on the topic of GPS Jamming. This item was first broadcast in August 2013 on BBC Radio 4 and was subsequently networked through the BBC World Service.

C.2 FOX NEWS REPORT - 2012

http://www.foxnews.com/tech/2012/02/23/gps-emerging-threat/

This is an excellent Fox News piece put together during the GPS Vulnerabilities conference held at NPL UK in Feb 2012 with an interview with Todd Humphreys who gave the Keynote presentation.

C.3 BLOOMBERG - GPS JAMMERS THREATEN AIR TRAFFIC NAVIGATION – 2012

http://www.bloomberg.com/video/88574724-gps-jammers-threaten-air-traffic-navigation.html

This is a good report by Bloomberg on the impact of cheap GPS jammers on Newark story. It also refers to the Lightsquared story.

C.4 TED TALK: TODD HUMPHREYS: HOW TO FOOL A GPS - 2012

http://www.ted.com/talks/todd_humphreys_how_to_fool_a_gps.html

This is a really good piece by Todd Humphreys given during a TED talk in Feb 2012

C.5 FOX NEWS REPORT ON SPOOFING -2013

http://www.foxnews.com/tech/2012/06/25/drones-vulnerable-to-terrorist-hijacking-researchers-say/

Todd Humphreys conducted spoofing research using a small radio controlled helicopter.

C.6 GPS FOR HUMANITY -- THE STEALTH UTILITY - 2013

http://www.ustream.tv/recorded/30187681

The story behind how GPS was conceived by Col. Brad Parkinson given at the Smithsonian National Air and Space Museum in March 2013.

C.7 DUBAI AIRSHOW 2011 – MAXIM ANTONOV OF AVIOCONVERSIYA EXPLAINS JAMMERS

http://www.ainonline.com/aviation-news/blogs/ain-blog-gps-jammer-guy-touts-wares-dubai-air-show

APPENDIX D SYMPOSIA AND CONFERENCES FEATURING SENTINEL PRESENTATIONS

2011

D.1 COUNTER TERROR EXPO, LONDON

Protection of Critical National Infrastructure from GPS Jamming and Interference (available here)

D.2 DSEI 2011, LONDON (INTERNATIONAL EVNT)

Improving the Security and Safety of PNT based Applications and Critical Infrastructure by detecting and locating sources of interference to GNSS (available here)

D.3 NAVWAR MOU MEETING, UK (INTERNATIONAL AUDIENCE)

GNSS Interference and Detection SENTINEL/GAARDIAN

D.4 UK SPACE AGENCY SECURITY AND RESILIENCY UNIT

Presentation

D.5 JOINT NAVIGATION CONFERENCE 2011, USA (CLASSIFIED)

Presentation

D.6 ASSOCIATION OF CHIEF POLICE OFFICERS: INTERNATIONAL CONFERENCE OF FORENSIC INVESTIGATORS

D.7 INSTITUTE OF NAVIGATION (ION) CONFERENCE 2011, USA (INTERNATIONAL EVENT)

Improving the Security and Safety of PNT based Applications and Critical Infrastructure by detecting and locating sources of interference to GNSS (available here)

D.8 EUROPEAN NAVIGATION CONFERENCE (INTERNATIONAL EVENT)

Exhibition and presentation

D.9 SPACE WEATHER CONFERENCE, FRANCE

Presentation

D.10 OTHER

Regular briefings to ACPO and updates to UK Homeland Security throughout 2011

2012

D.11 INTERNATIONAL CONFERENCE OF FORENSIC INVESTIGATORS (ICCDF), LONDON

Presentation

D.12 KTN GPS JAMMING CONFERENCE, NPL, TEDDINGTON, LONDON

Presentation

D.13 OFCOM ADCO R&TTE MEETING

Presentation

D.14 GNSS VULNERABILITIES CONFERENCE

Presentation

D.15 INTERNATIONAL COMMITTEE ON GNSS WORKSHOP, VIENNA

Presentation

D.16 EUROPEAN GNSS AUTHORITY PRS WORKSHOP

Presentation

D.17 CABINET OFFICE BRIEFING ON GNSS VULNERABILITY

Presentation

D.18 JOINT PRESENTATION BY NATS AND CAA ON GNSS RESILIENCE, LONDON

Presentation on GNSS interference and proposed monitoring activity to British Air Line Pilots Association (BALPA) Technical Committee, Heathrow.

D.19 NATS: ICAO NAVIGATION SYSTEM PANEL (SPECTRUM SUB GROUP), MONTREAL

Presentation to experts nominated by ICAO Member States and their advisors on aviation navigation issues

D.20 NATS: EUROCONTROL RNAV APPROACH IMPLEMENTATION SUPPORT GROUP (RAISG)

Initial briefing to European Air Navigation Service Providers, Regulators (Technical Operational) Aircraft Operators, Avionics suppliers, US Federal Aviation Administration, Eurocontrol and GNSS Supervisory Agency

D.21 GSA PRS MEETINGS, BRUSSELS

Presentation

D.22 CGSIC INTERNATIONAL MEETING, NASHVILLE, TENNESSEE, USA

Presentation of SENTINEL results

D.23 KTN: RESILIENT PNT, NPL TEDDINGTON, LONDON

Presentation

D.24 ITSF 2012, NICE, FRANCE

Presentation on GNSS Vulnerabilities

2013

The SENTINEL research project was showcased in five different countries by three different presenters in the space of seven days during April 2013, underpinning the global importance of this research. Additionally, it was presented:

D.25 TRANSPORT RESEARCH LABORATORY

Presentation

D.26 CHATHAM HOUSE - CYBER & SPACE SECURITY WORKSHOPS - JAN & MAY

Presentation

D.27 KTN LOCATION & TIMING EVENT: GPS JAMMING & MITIGATION, UK

Presentation

D.28 SECURITY & POLICING, UK

Presentation of SENTINEL to James Brokenshire, Minister for Security

D.29 WSTS, SAN JOSE, CALIFORNIA, USA

Presentation – GPS Vulnerability, highlighting the potential threat that GPS jamming might have to the next generation of mobile telecoms networks if appropriate mitigation technology is not considered during the critical infrastructure roll out phase

D.30 ICG WORKSHOP, HONOLULU

Presentation by Prof. David Last at the ICG Workshop prior to the ION Pacific PNT Conference

D.31 EUROCONTROL, BRUSSELS, BELGIUM

Presentation of the SENTINEL project. This Conference quantified the threat posed to airports where GPS based landing technology is under consideration for adoption to assist landing operations.

D.32 DISRUPTIVE TECHNOLOGIES, UK

Presentation

D.33 USNO, NAVIGATION & TIMING SYMPOSIUM, WASHINGTON DC, USA

Presentation updating the SENTINEL project and illustrating the results of GPS jamming which was delivered by Prof David Last, a recognised global expert on GPS and eLoran technology. GPS jamming is as much of a challenge in the US as it is in the UK.

D.34 ROYAL AERONAUTICAL SOCIETY – FUTURE WEAPONS, FARNHAM, UK

Presentation

D.35 SECURITY EVENT, NETHERLANDS

Invitation to present on GNSS Vulnerabilities by the Dutch Police

D.36 CGSIC, NASHVILLE, TENNESSEE, USA

Presentation, Update on SENTINEL

D.37 SPRINT WORKSHOP ON SYNC & TIMING, KANSAS, USA

General presentation on GNSS Vulnerabilities

APPENDIX E ACRONYMS AND ABBREVIATIONS

Acronym	Description
ACPO-ITS	Association of Chief Police Officers – Intelligent Transport Systems
CRPA	Controlled Radiation Pattern Antenna
CSAC	Chip Scale Atomic Clock
ECD	Envelope to Cycle Difference
EGNOS	European GPS Navigation Overlay Service
eLoran	Enhanced Loran - a Low Frequency trans-national PNT service
GAARDIAN	**G**NSS **A**vailability **A**ccuracy **R**eliability an**D** **I**ntegrity **A**ssessment for timing and **N**avigation
Galileo	The European global navigation satellite system
GBAS	Ground Based Augmentation System
GLAs	The General Lighthouse Authorities of the United Kingdom and Ireland
GNSS	Global Navigation Satellite Systems
GPS	Global Positioning System
IEEE	The Institute of Electrical and Electronics Engineers
ITU G.811	International Telecommunication Union - PRC Standard for Telecom Networks
ITU SG15/Q13	International Telecommunication Union - Study Group 15, Question 13
IDM	Interference, Detection & Mitigation
LEA	Law Enforcement Agencies
LTE-TDD	Long Term Evolution – Time Division Duplex
M2M	Machine-to-Machine
MTIE	Maximum Time Interval Error
NATS	National Air Traffic Services
NPL	National Physical Laboratory
OCXO	Oven Controlled Crystal Oscillator
OS	Ordnance Survey
PNT	Positioning, Navigation & Timing
PRC	Primary Reference Clock
PTP	Precision Time Protocol as defined in the IEEE 1588 Standard
QoS	Quality of Service
RFI	Radio-Frequency Interference
SBAS	Space Based Augmentation System
SENTINEL	GNSS **SE**rvices **N**eeding **T**rust **I**n **N**avigation, **E**lectronics, **L**ocation & timing
SNR	Signal-to-Noise Ratio
SWaP	Size, Weight and Power
TIE	Time Interval Error
TOA	Time of Arrival
TRL	Technology Readiness Level
UoB	University of Bath
USNO	US Naval Observatory
UTC	Universal Coordinated Time