GNSS denial: a real and present danger?

An irritating inconvenience? Or a global menace? In the first of a two-part article, GEOconnexion looks at the evidence, and at the latest developments to safeguard satellite navigation services

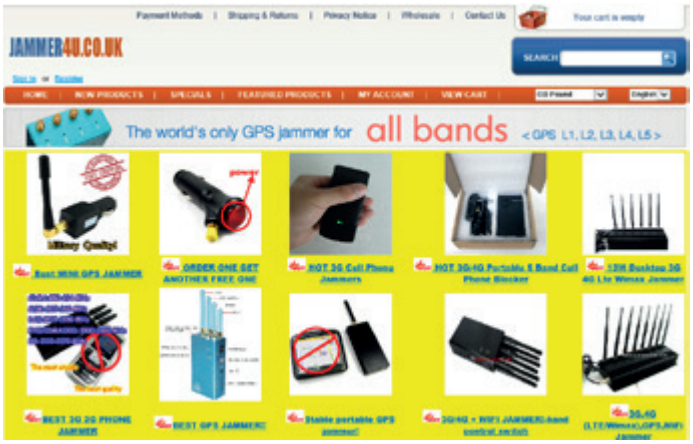
Motorists travelling north of Seoul on the morning of 23 August 2010 were perplexed as guidance from their satnav systems faltered and then cease entirely. For the next two days, signals from the 31-strong constellation of GPS position-fixing satellites were rendered virtually inaccessible across swathes of the Korean peninsula for up to 10 minutes at a time. It posed problems for Air Traffic Control and shipping, created havoc for delivery services, and generated a major headache for the country's military.

While North Korea denied responsibility for the turmoil, subsequent investigation revealed that high powered jamming from Kaesong, just north of the 38th parallel, was almost certainly the culprit. South Korea's defence minister, Kim Tae-young, told members of the National Assembly that the jamming posed a "new kind of threat" and cited an intelligence report which claimed the North Koreans had vehicle-mounted devices capable of jamming GPS signals within a radius of 50 to 100 kilometres. Whatever the truth of the matter, it has gone down in history as the first recorded attempt at GNSS (Global Navigation Satellite System) denial. Nor was it the last, with further disruptions occurring in March 2011 and April 2012, with outages lasting up to 16 days.

Vulnerable signals

The relatively weak L-Band signals transmitted by GNSS constellations such as America's GPS, Russia's GLONASS, China's BeiDou and Europe's Galileo make them particularly vulnerable to man-made interference. And while wide area Radio Frequency jamming requires powerful transmitters, the ease with which the technology can be miniaturised has seen a proliferation of cheap mail order devices on offer to drivers who seek to block trackers fitted to fleet vehicles and to criminals who use them in pursuit of high-value vehicle theft. The more tech-savvy can build their own jammers from a variety of online circuit diagrams and instructions.

Yet even these devices, ranging in size from cigar lighter plug-ins to desktop units and with power outputs up to two watts and with



Just one of many offshore web sites offering low-power GPS jammers to UK consumers

shielding up to a radius of 300 metres, can seriously impact on the safety of those who depend on accurate positioning, whether on land, at sea, or in the air. The advent of autonomous vehicles raises the safety stakes even higher.

There is an economic cost too. It is estimated that more than 3.3 million jobs in the United States rely heavily on GPS, generating approximately US$122.4 billion in annual economic benefits.[1] Needless to say, any widespread disruption to services would prove costly. A report issued by NDP Consulting Group in 2011 noted that the direct economic costs of full GPS disruption to commercial GPS users and GPS manufacturers would amount to some US$96 billion per year, equivalent to 0.7 percent of the U.S. economy.[2]

Europe, too, is now heavily reliant on GNSS, with the European Commission estimating that €800 billion of the European economy now depends on such services.3 Hardly surprising when one considers the range of applications served; from transport to construction engineering, from precision farming to cashpoint machines, and from surveying and mapping to telecommunications. And while positioning and navigation are key services provided, GNSS atomic clock timing signals are equally critical, e.g. for cellular communications; for time-stamping transactions in global financial markets, and for synchronising smart power grid operations. It adds up to a €183bn global market for GNSS devices, a sum that is expected to increase by 8.3% annually up to the end of the decade with some seven billion devices then in use.[1]

It is against this background that governments around the world are taking the threat of disruption seriously, with many imposing swingeing fines on those advertising, selling or illegally using jammers. In the UK, the domestic sale, installation and use of GNSS jammers is prohibited although their offshore purchase, importation and possession is not.

While GPS jammers can be found on auction sites for as little as £15, the tech-savvy can build their own from web-accessible circuit diagrams and instructions

Detection

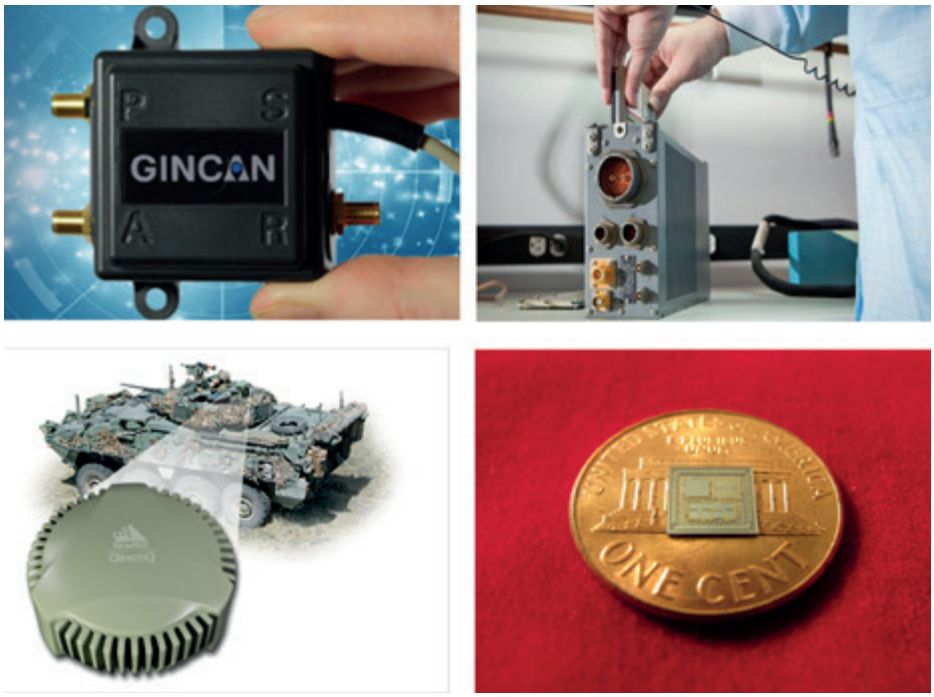
Of course, law enforcement depends on the timely detection and location of GPS jammers and a variety of detectors are becoming available for this purpose. A new system from Exelis Geospatial Systems that locates GPS interference sources in 3-D, completed a series of tests at the UK's Defence Science and Technology Laboratory towards the end of last year. Based on a network of threat-detection sensors and proprietary location algorithms, the Signal Sentry 1000 successfully detected and located both stationary and moving jammers in a variety of environments.

More portable solutions have been pioneered by UK-based Chronos Technology with its low-cost CTL3510 detector/locator and its more versatile and sensitive stablemate, the MIRA-tested CT3520 with visual display. Both handheld, battery-operated units will detect and locate jamming signals in the GPS L1 band and can discriminate against false alarms from local multipath or interference and determine multiple jamming event patterns over time. The developments benefit from the company's long-term involvement in two Technology Strategy Board (now Innovate UK) flagship research projects – GAARDIAN and SENTINEL - into GPS jamming.

Countermeasures

Efforts are also underway to make satellite navigation signals less sus-

(Left): The Exelis Signal Sentry 1000 user interface supports timely and effective actionable intelligence in GPS denied and contested environments (Image: Exelis Ic.), while (Right) handheld units from Chronos Technology will detect and locate jamming signals in the GPS –L1 band (Photo: Chronos Technology)



Examples of anti-jam developments (from top left clockwise) Chemring Technology Solutions' GINCAN GPS detection and anti-jam device measures just 48x24x24 mm (Photo: Chemring Technology Solutions). Raytheon's anti-jamming GPS avionics receiver (Photo: PR NewsFoto/Raytheon). As part of DARPA's Micro-PNT program, researchers at the University of Michigan have fabricated a prototype Timing & Inertial Measurement Unit (TIMU) that integrates a six-axis IMU (three gyroscopes and three accelerometers) and a highly-accurate master clock on a single chip (Photo: DARPA). The GAJT anti-jam antenna from NovAtel and QinetiQ is an externally-mounted vehicle unit that requires only power and a single RF cable (Image: NovAtel Inc.)

ceptible to malicious or unintentional interference, e.g., Europe's Galileo system will employ an encrypted Public Regulated Service to protect signal availability and data flows to law enforcement agencies, customs authorities and the emergency services. The US defence research agency, DARPA, has set up a dedicated Micro-Technology for Positioning, Navigation and Timing (Micro-PNT) program to develop microchips that "know" their position in space and time independently of satellites.

Although some way off for general use, affordable anti-jamming devices for GNSS receivers are currently under development. For example, Chemring Technology Solutions unveiled GINCAN, the world's first miniaturised GPS detection and anti-jam unit, at the Security and Policing Show in Farnborough earlier this year. Across the Atlantic, tests conducted last year by the US Air Force at the White Sands Missile Range succeeded in maintaining GPS satellite tracking and navigation at jamming levels far exceeding technical requirements. These tests utilised Raytheon's Miniaturised Airborne GPS Receiver 2000 equipped with a specialised M-code receiver card and coupled to an Advanced Digital Antenna Production (ADAP) system. Component-level developments are also underway, with Orlando-based MtronPTI announcing two new filters - the LF9454 and LF9455 - intended for GPS receivers fitted to battlefield UAVs. These filters maintain satellite lock by blocking jammer signals around the two primary GPS bands. Also intended for battlefield use is GAJT-700ML, a development from NovAtel and QinetiQ which claims to be the first single unit anti-jam antenna. Field-tested last year by the Canadian Army, this M-Code-ready COTS product is aid to be easily integrated into new vehicle platforms or retrofitted with existing GPS receivers.

First trialled in 2007 and rolled-out operationally from 2013, the GLAs eLoran service now serves shipping heading for seven British ports and provides positional information accurate better than 20 metres

Alternatives

In the meantime, land-based backups to GNSS are being pursued, most notably by South Korea which is currently implementing a US$12 million differential eLoran low frequency radio navigation system to cover its coastal waters to an accuracy of 20 meters. While the first phase of this development is unlikely to be operational before 2018, the General Lighthouse Authorities of the UK and Ireland (GLA) has already implemented eLoran as a backup to GPS for shipping on Britain's busy east coast.

The GLA is also supporting an industry initiative to operate eLoran on a commercial basis across Europe, and working with Russia to make that country's legacy Chayka (Seagull) radio navigation system interoperable with eLoran for vessels negotiating the Arctic route from the Far East. Elsewhere in Europe, the Dutch Pilots' Association, Nederlands Loodswezen, is developing an eLoran system to ensure safety and smooth traffic flows in the approaches to Rotterdam, Europe's busiest seaport.

Radar-based position fixing alternatives to GNSS have also been proposed for busy waterways, not least by Russell Technologies of Canada which has developed its XIR3000 digital radar processor unit as an add-on to most contemporary radar transceivers. This further evolution of the RadarFix system developed in the late 1980s by Helmut Lanziner works with onshore radar reflectors and other fixed targets to obtain accurate range and bearing measurements. This information, together with a radar image overlay, is displayed on an electronic chart to display a vessel's movement in real-time and to an accuracy of around two meters depending on the number of targets.

Issues of GPS vulnerability were very much on the minds of those attending this year's Institute of Navigation conference in Manchester and where a succession of speakers highlighted the latest efforts being made to detect and mitigate interference with satellite signals. We will be exploring those cutting-edge developments in our next issue

1,2. GPS Jamming: Out of Sight, The Economist, 27 July 2013
3. GNSS Market Report 4. European Global Navigation Satellite Systems Agency. March 2015