Navigating the Future:

GNSS and the Future of Satellite Navigation Technology

RAPPORTEUR: JOHANNA SYMMONS

To most people satellite navigation is synonymous with the devices attached to the dashboards of their cars. But without global navigation satellite systems (GNSS), you couldn't track your Fedex shipments, rescue services would take perilously longer to reach emergencies and banks would likely foul up billions in stock trades. GNSS is now a near-universal utility, providing vital positioning, navigation, and timing services to both consumers and businesses; and the technology is today critical to everything from speed cameras and digital radio to ship-docking and farming– not to mention finding the nearest Starbucks on an iPhone.

With the aim of offering a comprehensive primer on the technical, legal and commercial issues raised by GNSS technology, the London Institute of Space Policy and Law, together with the law firm Bird & Bird, the Royal Institute of Navigation and the Society of Satellite Professionals International (SSPI), jointly hosted a seminar on the subject in London on 14 July 2010.

1. GNSS PROJECTS

1.1 New Kids on the Block

After an introduction by Bird & Bird partner Graeme Maguire, senior associate Richard Graham summarised existing and planned global navigation satellite systems.

The best-known and most widely used GNSS is the Global Positioning System (GPS), a network of satellites run by the US military and available free-of-charge for commercial use since 1994. This "dual use" is the system's major downside: in times of conflict, Washington might seek to protect its own military or strategic interests by restricting the technology's signal strength or accuracy – or even by shutting down public access entirely.

With the geopolitical stakes in mind, other major powers have been muscling into the game by launching their own GNSS: Russia is revitalising Glonass, a network it launched in 1982, while China plans to introduce a system called Compass. Europe, meanwhile, is pressing ahead with its own system, Galileo, which the European Commission expects will be operational by 2014, despite numerous funding setbacks.

According to Graham, the next generation of GNSS will involve multiple stakeholders – both upstream and downstream - and could, in the EU alone, create a market for satellite-based navigation services worth several hundred billion euros.

1.2 Interoperability

Most receivers today are exclusively GPS-compatible, but with the advent of new GNSS, this will change. Technical solutions for interoperability are already on their way, according to Cockshott. Many receiver chips will be Glonass-compatible by the

end of 2011 “but you won’t even know,” Parsons said. From the satellite operators’ viewpoint, agnostic receivers for multiple systems are a drain on battery, but otherwise not a problem, said Ann Vandenbroucke, head of regulatory and policy issues at satellite operator Inmarsat.

2. TECHNICAL ISSUES

Professor Andy Norris, chairman of the Royal Institute of Navigation’s Technical Committee, reviewed some of the technical issues facing GNSS. He highlighted in particular the hotly debated issue of “jamming”, where receivers are deliberately blocked from getting signals.

2.1 The More the Merrier?

Given GPS’s primacy today, the consequences of system failure could be catastrophic, particularly for the emergency services which rely heavily on GPS.

There is therefore a rationale for developing alternative systems to GPS. But although in general “the more [systems] the merrier”, Norris warned that the simultaneous disruption of multiple systems is not impossible because all systems suffer from the same shortcomings, namely: weak signals, similar operational frequencies and the need for a direct line of sight between the satellite and the receiver, which poses a problem for indoor use.

The position performance of any GNSS could be undermined by natural or man-made events including solar storms, “urban canyons”, interference from other electronic systems and intentional obstructions such as jamming or spoofing.

2.2 Solar Storms

Natural events such as solar storms pose a risk to GNSS reception because they could damage satellite electronics and disable all signals, even permanently. Fortunately powerful solar storms do not happen often, Norris noted. But if solar activity picks up in coming years as some scientists now predict, the risk to satellites would increase.

2.3 Urban Canyons

Although many GNSS users live in urban areas, the systems function poorly in cities – often referred to as “urban canyons” – where buildings degrade accuracy. GNSS systems also do not work well indoors. Vandenbroucke of Inmarsat recounted how a taxi driver almost lost his way in a multi-storey car park despite using two sat nav devices simultaneously.

Integrating GNSS with other location technology is a possible solution to this problem. Google uses a hybrid approach, relying on a mixture of GPS and radio, which works well in urban areas, according to Ed Parsons, the firm’s geospatial technologist. The company has built databases of cell towers and can thereby approximate position up to100m accuracy. By then mapping data to a wi-fi hotspot list, it can achieve accuracy up to10m.

Multiple GNSS will not eliminate the urban canyon problem. However, there will be somewhat better performance for receivers that use satellites from a number of systems, said Bob Cockshott, director of the Location and Timing Programme at Digital Systems KTN, an organisation funded by the Technology Strategy Board to promote the UK's economic growth.

2.4 Unintentional Interference

As the GNSS signal is weak, unintentional interference with its radio spectrum from external sources, in particular ones sharing the same frequency allocation, could compromise it, a seminar participant noted. Russia, for example, will not allow Globalstar mobile satellite services to be installed on its aircraft because they are fundamentally incompatible with
Glonass, which operates in a portion of the frequency band allocated to Globalstar for user uplinks.

Ultra-wide band communications systems can be particularly problematic and in cases of close spectral proximity, filtering is often unable to eliminate the problem. As a solution another seminar participant proposed new receivers capable of superior filtering, but conceded that introducing tough spectral masks will take time.

"Spectrum is a policy orphan", Vandenbroucke said. Few policymakers take an interest and "politicians have no idea of interference problems. [We] need to say that GNSS are weak systems, and need to be protected."

Graham explained that access to spectrum – a finite resource - is a highly political issue. This is exemplified by China's plans to use some of the same frequencies as Galileo for its Compass system. The EU, which has reportedly offloaded Chinese-built hardware from the Galileo satellites, is now in discussions with China about spectral separation.

2.5 Jamming and Spoofing

Jamming – the deliberate use of devices to block receivers from getting signals – raises a number of security concerns as GNSS proliferates, not least because jamming devices are very easy to come by, Norris warned.

GNSS jammers are cheap, easy to develop, function on minimal power and can be picked up without much hassle online. This contrasts with jammers for many other electronic systems which tend to be expensive and difficult to build, meaning that beyond military use, there is often little incentive to develop or acquire them.

GNSS jammers are often used for stealing vehicles fitted with GPS-based tracking systems; recent high-profile cases include the organised theft of a number of prestige cars in the UK. People also use jammers to prevent detection by vehicle-tracking systems used by companies to keep tabs on employees. The devices could have numerous other illicit uses, including breaking GNSS-tagged home detention sentences or restriction orders and dodging future road charges.

While military systems are designed to resist jamming, the potential impact of jammers on civilian infrastructure could be severe: in a coastal test, a low-power, 1.5 watt device jammed GNSS receivers up to 30km out to sea, Norris noted. This caused havoc for ships in the area, many of which experienced a complete loss of positioning. One ship's GPS system, rather than warning of a possible malfunction, claimed the ship was landlocked in Northern Ireland.

According to Norris, the International Maritime Organisation (IMO) is set to discuss the issue of jamming with the UK Maritime and Coastguard Agency (MCA), which it advises. It is also looking at requiring ships to fit better receivers.

Seminar participants agreed that more sophisticated GNSS receivers could offer a technological solution to jamming. Such receivers could incorporate antennae that eliminate jamming or technology such as Receiver Autonomous Integrity Monitoring (RAIM) to alert users that their receivers are being jammed. Norris also suggested back-up positioning systems that are not satellite-based.

Aside from simply jamming GNSS, it is also possible to "spoof" it – that is, to transmit synthesised satellite signals which blot out the real ones and cause a nearby GNSS receiver to indicate a false location of the spoofer's choice. GNSS spoofers are now within the reach of organised crime and could, in the hands of terrorists, pose an even greater threat to security than jammers, said Cockshott at Digital Systems KTN.

The relevant question for the law is whether law enforcers need better detection systems and whether penalties for jamming and spoofing should be strengthened. "The problem is, you're always catching up. It's difficult to be prescriptive," Maguire said.

3. LEGAL ISSUES

Inmarsat's Vandenbroucke laid out some of the regulatory and policy issues raised by GNSS, highlighting in particular the issue of liability. Google's Ed Parsons brought the question of privacy to the debate. Bird & Bird's Graham said that privacy is an easier legal issue because culprits are readily identifiable whereas liability is "the elephant in the room".

3.1 Liability

All GNSS service users, and rescue services in particular, want to be able to rely on accuracy, availability and coverage of their GNSS at all times. However, at present, there is no simple answer to who is liable if the service fails in these respects. As Cockshott pointed out, GPS is free, but it lacks guarantees at service level – and suing the US military would likely prove difficult. The proposed Galileo system may offer a fee-based and guaranteed Safety of Life service, but the question of who is liable in case of failure remains.

Vandenbroucke noted that for GNSS, the chain of responsibility is long and international, ranging from the satellite manufacturer, the GNSS operator and the oversight authority to the terminal provider, the application provider and the end user.

This not only makes it difficult to ascertain liability, but also opens the door to conflicts of law.

Inmarsat initially expressed interest in being an operator within the Galileo project, but in light of liability (and intellectual property) issues, dropped out of the consortium, Vandenbroucke said.

Given the uncertainty surrounding the question of liability, insurance costs could escalate to the point where GNSS operators become uninsurable. This begs the question of whether traditional insurance mechanisms are sufficient. One solution may be for the government to shoulder some liability while other options could include a part government/part commercial insurance pool or a new treaty exclusion of liability in all jurisdictions, Vandenbroucke pointed out.

Sa'id Mosteshar, director of the London Institute for Space Policy and Law, asked whether multiple operators would help reduce liability. Bird & Bird's Graham responded that while there is less of a chance that things go wrong on the technological front, multiple operators would complicate the blame game even further. "Hopefully," added Maguire, "[the different systems] won't go wrong at the same time."

3.2 Privacy

Thanks to GNSS, we will always be able to know where we are and, in theory, our children should never get lost, said Google's Parsons. But he also noted the flipside: other people will also know where we are. As position becomes an integral part of social networking and, ultimately, user identity, public concerns over privacy are growing, said Cockshott, even though the GNSS privacy debate is still in its infancy.

While Parsons admitted that Google – which is under investigation by the UK's privacy watchdog for gathering private information when setting up its Streetview service – may recently have been "a bit too enthusiastic" in collecting data, he stressed that the company's aim is to deliver services that provide "context" – that is, wider information linked to a particular location. Through this so-called ambient location technology, Google hopes to provide its customers with information, for example, on the location, opening hours and stock prices of businesses catering to their interests. You would also be able to find the most efficient way home from, say, a Justin Bieber concert where 80,000 other fans are clogging the roads.

Parsons cautioned that the notion that location in itself constitutes personal information is unclear and has yet to be established by case law. Moreover, he argued that a person's location *per se* is generally not at issue, but rather the combination of location and other data that together make up personal information.

Despite the legal uncertainty surrounding the use of location information, Google is following best practice to ensure transparency around privacy, Parsons said. The company asks users to "opt in" for location data gathering and sends a reminder to this effect every six weeks. But he warned that it's only a matter of time before a celebrity who has been tracked brings the case to court.

By contrast, the public is generally less aware of the government's gathering of location data. Parsons said there have been over 100,000 instances of such information being made available to US law enforcement agencies over a six month period alone.

Relying on government to protect our privacy "is like asking peeping Tom to install window blinds," Vandenbroucke said. Since 9/11, it has become standard procedure for any satellite operator seeking a licence to allow government access to information under certain conditions.

Separately, Vandenbroucke noted that although there is a vast body of law on data retention and protection, different jurisdictions have distinct and sometimes conflicting requirements for data back-up systems, which can be an issue for international satellite operators.

4. COMMERCIAL ISSUES

According to Graham, "everyone is a GNSS stakeholder" – from satellite operators upstream to the service providers downstream. The marketplace is potentially enormous, with estimates for the EU alone in the hundreds of billions of euros. According to Parsons, sales of GPS-enabled smartphones have risen 90% year-on-year.

However, one problem raised by speakers was how stakeholders would make money through GNSS. GPS is freely available for commercial use, while under Google's business model, mobile devices provide free applications: how can other business models compete?

The question is particularly pertinent with regard to Europe's Galileo GNSS, which hopes to provide better accuracy than GPS and plans to generate income from premium services that rely on encoded signals.

However, the Financial Times Deutschland in October cited a European Commission report as saying Galileo will be unprofitable "over the long term", running at an annual loss of 750 million euros.

Some estimates suggest Galileo will cost taxpayers 20 billion euros over the next 20 years. The GNSS was supposed to be built and operated by a public-private partnership (PPP), but attempts to negotiate a Galileo concession agreement with a private consortium of aerospace companies collapsed in 2007 and it was decided to proceed with Galileo as a purely public undertaking.

Inmarsat dropped out of the private consortium interested in forming the Galileo concession holding company due to concerns over liability and intellectual property. Inmarsat does, however, contribute to the European Geostationary Navigation Overlay System (EGNOS), which is Europe's first activity in the field of GNSS and a precursor to Galileo. EGNOS is a satellite-based augmentation system (S-BAS) which enhances existing GNSS such as the US GPS and the Russian GLONASS and makes them suitable for safety-critical applications such as flying aircraft or navigating ships through narrow channels.

According to Vandenbroucke, Inmarsat provides space capacity for S-BAS by means of a dedicated satellite channel, or transponder. This works like leasing space on a building: the GNSS payload is “piggybacked” onto the satellite’s main payload. Inmarsat’s business model has evolved from simply leasing space on a satellite into a fuller package which also integrates the use of ground stations, which send or receive data to and from orbiting satellites.

Vandenbroucke pointed out that many of Inmarsat’s customers use augmented services for critical services such as safety and rescue, and that Inmarsat plays a crucial role in providing spectrum allocation efficiency. “GNSS is to Inmarsat what GPS is to Vodafone”, she said.