



## **GPS pioneer warns on network's security**

BY: SAM JONES and CAROLA HOYOS

*Financial Times*

13 February 2014

The Global Positioning System helps power everything from in-car satnavs and smart bombs to bank security and flight control, but its founder has warned that it is more vulnerable to sabotage or disruption than ever before – and politicians and security chiefs are ignoring the risk.

Impairment of the system by hostile foreign governments, cyber criminals – or even regular citizens – has become “a matter of national security”, according to Colonel Bradford Parkinson, who is hailed as the architect of modern navigation.

“If we don’t watch out and we aren’t prepared,” then countries could be denied everything from ‘navigation’ to ‘precision weapon delivery’, Mr Parkinson warned.

“We have to make it more robust ... our cellphone towers are timed with GPS. If they lose that time, they lose sync and pretty soon they don’t operate. Our power grid is synchronised with GPS [and] our banking system.”

Western governments are “in their infancy in recognising the problem”, Mr Parkinson told the Financial Times in an interview on the fringes of a conference for government officials, academics and defence contractors at the UK’s National Physical Laboratory.

He said: “[In the US] I don’t know anyone that is really in charge of it. The Department of Homeland Security should be [but] ... they don’t have any people that understand it very well. They’ve got one person without any budget to speak of.”

Mr Parkinson, now a professor at Stanford University, created GPS in the 1970s on behalf of the US military – who still control the system of satellites today.

Use of the system for civilian purposes has exploded with the development of mobile technologies. Though the US military has in place protection that could give its navigation systems a high-degree of robustness, most civilian GPS systems have none, Mr Parkinson said. He also warned that the EU’s new €5bn Galileo satellite system, created as an alternative to the US-controlled GPS, was equally at risk. Richard Peckham, who helped develop the Galileo system, said that although its public service was encrypted, making it more difficult to hack and more secure for users such as the emergency services and public utilities, it was still vulnerable to jamming and interference.

The US, which initially opposed the European satellite constellation, has come around to supporting it, in part because Washington has realised it needs a GPS back-up system that is neither Russian nor Chinese.

A report compiled for the UK government and released this week warned that “the conditions are present for a catastrophic ‘Black Swan’ event” that would knock out one or more critical GPS systems. The report identified thousands of instances of GPS jamming occurring annually.

Disruption of satellite navigation systems has so far remained a relatively low-level problem for governments. Small-range jamming devices can be acquired easily via the internet. However, more powerful jamming equipment is becoming increasingly easy to acquire.

Over the past few years South Korea has witnessed huge jamming attacks against its GPS systems, launched by North Korea. The areas affected stretch 100km into South Korean territory, and include major airports and shipping lanes. More than 1,000 ships and 250 planes had their travel disrupted by North Korean jamming attacks in 2012.

Seoul has responded by ordering the construction of a land-based antenna array over more than 40 sites to provide a back-up system.

The UK has already begun to build a similar system, primarily to help shipping in the event of GPS disruption. The stretch of water between Britain and France is one of the busiest shipping lanes in the world, but navigation throughout it could be disrupted by a single portable jamming device.

“When a ship loses GPS, it isn’t like a car satnav,” said Professor David Last, a consultant to the UK’s General Lighthouse Authority. “Multiple systems fail simultaneously.”

Prof Last cited a report into navigation vulnerabilities from the Royal Academy of Engineering that found “there was barely a single area of commerce or industry in the UK that wasn’t dependent on GPS in some way.”