SPACE: THE FINAL FRONTIER

Nigel Davies *predicts that Global Navigation Satellite Systems will become a key battleground of the future*

The implications of recent developments are clear; space will form a key terrain of future conflicts as Global Navigation Satellite Systems (GNSS) come under increasing attack.

In 2016, North Korea launched an unprecedented month-long attack on its neighbour, South Korea, using powerful radio waves to drown out Global Positioning System (GPS) signals, forcing ships to return to port, causing chaos on the roads, disrupting commercial flights and impacting mobile phone coverage. GNSS jamming has also played a key role in the recent Ukraine conflict. Russia recently used the Krasukha-4 – a truck-mounted broadband multi-functional jamming station – to block communications systems and spy satellites over Ukraine, shrouding Russia's activities in an electronic cloak that blinded and muted its enemies. The Organisation for Security and Cooperation in Europe (OSCE) was even forced to abandon reconnaissance missions over Ukraine when its monitoring drones came under sustained attack from high-powered satellite jammers. Electronic jamming presents a major threat to unmanned aerial vehicles (UAVs) and unmanned ground vehicles (UGVs) because, without humans at the wheel, they rely entirely on sensors and satellites for safe navigation.

Western powers are now rushing to join the electronic arms race: last summer the US warned aircraft of potential disruption to their flight stability controls and GPS readouts when it began testing enormous airborne GNSS jamming weapons over the Naval Air Weapons Station at China Lake, California. Ofcom has also issued notifications warning of GPS jamming exercises by the Ministry of Defence (MOD).

However, the technology is not confined to nation states. Handheld jammers with significantly less power and a smaller range can still knock out satellite signals across an area of an airport, forming an attractive weapon for non-state actors, including terrorist groups. These devices are widely available for sale on the internet and criminals are increasingly using them often to evade detection by police or employers. The NSL Strike3 Project – an international investigation into GNSS threats funded by the European GNSS Agency – recorded 400 GPS jamming interference incidents at a single airport, 138 incidents on a motorway and 839 in an inner city location in one week alone.

We are already seeing new threats to satellite navigation systems beginning to populate the battlefield. GNSS 'spoofing' involves echoing GNSS signals with counterfeit signals, which provide a false time and position. In 2013, a group of researchers from the University of Texas demonstrated how they could lead a 213ft yacht off course by echoing genuine GPS signals that duped the autopilot. This highlighted how the danger is even greater for unmanned vehicles that have no human pilot.

In 2011, a US military drone was allegedly electronically 'hijacked' by counterfeit GNSS signals causing it to unintentionally fly into Iranian airspace, where it was captured. It has been claimed that an attack forced it to switch to autopilot and search for unencrypted civil GPS frequencies, which were then 'spoofed.' With at least 10 countries now thought to possess weaponised drones and UAVs also being employed to make vital medical deliveries, the fallout from future 'GNSS hijacking' of unmanned aircraft could be more severe and wide reaching.

ELECTRONIC JAMMING PRESENTS A MAJOR THREAT TO UNMANNED AERIAL VEHICLES

If this kind of attack were carried out on unmanned military assets such as 'drone tanks' or the next generation of unmanned military ships, it could cause them to send out hazardously misleading information, transmitting a 'ghost position' to nearby ports, military bases or control centres. False GNSS co-ordinates could deliberately lead unmanned craft into the path of hazards or enemy assets.

In future, entire satellite constellations could also be under threat. A Royal Academy of Engineering report has warned that: "The risk of a common mode failure affecting an entire GNSS constellation or even multiple constellations cannot be ruled out". Recent reports indicate that China and Russia are planning to cripple satellite constellations with missiles, lasers or cyber attacks. Lieutenant General David Buck, commander of Joint Functional Component Command for Space, a US Strategic Command unit, recently warned: "Russia views US dependency on space as an exploitable vulnerability and they are taking deliberate actions to strengthen their counter-space capabilities". He added that: "China is developing, and has demonstrated, a wide range of counter-space technologies to include direct-ascent kinetic-kill vehicles, co-orbital technologies that can disable or destroy a satellite, terrestrially based communications jammers and lasers that can blind or disable satellites".

A Chatham House research report, *Space: The Final Frontier for Cyber Security*, also warned of the threat of devastating cyber attacks against GNSS control systems, mission packages or satellite control centres.

The Galileo satellite navigation constellation

Picture credit: The European Space Agency

WHY IS THE THREAT GROWING?

Electronic warfare systems pose a growing threat because they provide an obvious means for poorer countries to cancel out the technological advantages of Western powers; something referred to as "asymmetric warfare". As Douglas Loverro, US deputy assistant defence secretary for space policy, recently said: "An advanced US satellite might cost upwards of $1 billion; missiles that could destroy such a satellite cost a few percent of that sum; co-orbital microsatellites cost even less". Even a very powerful GNSS jamming or 'spoofing' device costs significantly less than the conventional weapons and platforms they are designed to disrupt. Meanwhile, the advent of Software Defined Radio (SDR) technologies and the availability of the underlying GNSS open-access standards has, according to one expert, enabled "GPS attacks on a shoestring".

There is an ever-expanding array of modern military and civilian technologies, from precision-

guided 'smart munitions' to 'smart cities', that now rely on GNSS signals. Smart munitions depend on GNSS for precision guidance onto targets and, although they can revert to inertial navigation in the event of a jamming attack, this renders them significantly less accurate. GNSS signals are also fundamental to modern surveillance and communications systems, the designation of target co-ordinates and precision navigation of military platforms. This will only increase with the growing array of unmanned military vehicles operating across air, land and sea as virtually all unmanned systems use GPS position and timing technology. It is estimated that 90 percent of military equipment, platforms and systems now depend on GNSS for some aspect of their functionality and this is increasing.

IN 2011, A US MILITARY DRONE WAS ALLEGEDLY ELECTRONICALLY HIJACKED BY FAKE GNSS SIGNALS

Another critical vulnerability lies in the degree to which GNSS represents a potential 'single point of failure' across many supposedly independent communication and navigation systems. Sea trials have shown that a powerful GNSS jamming attack can simultaneously shut down the radar, gyrocompass, clock and communications systems aboard a ship because they all share a common dependence on GNSS data inputs.

This renders many countries vulnerable to a 'black swan event' – something out of the blue – affecting GNSS across a wide area and producing a domino effect across many interconnected aspects of military infrastructure. The scale of the danger was outlined by Doug Loverro: "If we lost GPS worldwide, most of our war fighters—in fact, all of our war fighters—would lose the ability to navigate and tell time and drop the precision munitions and do everything we do with GPS".

DEFENCE STRATEGIES

Implementing strategies and systems capable of defending against these threats will require governments and militaries to treat the threat to satellite navigation as seriously as other military threats, including cyber security. It will require recognition of the fact that our national and economic security is heavily dependent on the availability and integrity of GNSS data and that measures must be taken to protect it.

The key is to ensure mission-critical military or security assets can safely navigate and operate independently of interference when signals or frequencies are blocked.

Future receiver chip technology will use a range of satellite navigation frequencies and constellations, all within a wider suite of protective technology, to ensure continuity of service in the event that multiple frequencies or even an entire constellation is jammed. Crucially, drawing a position fix from the consensus among a range of GNSS inputs will enable them to spot rogue or 'fake' GNSS signals in the event of disruption to one satellite frequency or even an entire constellation. Europe's Galileo GNSS constellation also incorporates a secure satellite signal, the Public Regulated Service (PRS), to provide protected navigation for government-authorised users including military services.

QUALITY ASSURED

Receiver chip technology will be able to process 'quality-assured' satellite navigation data by receiving and processing an array of position and timing data from both secure and open-service signals, as well as other GNSS constellations including the Russian GLONASS and Chinese Beidou and space-based augmentation services (SBAS) such as WAAS and EGNOS.

Recent trials by the Ordinance Survey, QinetiQ and Nottingham Scientific Ltd (NSL) have demonstrated that encrypted satellite signals such as PRS can be processed via cloud computing so that any internet-connected device, including a smartphone, can now access ultra-secure satellite signals that were once only available to specialised devices This could make highly secure satellite navigation signals available to many personnel on the ground.

Other innovations are also in gestation. The Ministry of Defence's Defence Science and Technology Laboratory (Dstl) is even working on a 'quantum compass', which would operate at a subatomic level and would consequently be very hard to echo or disrupt.

QinetiQ is similarly exploring novel techniques using celestial navigation and even 'opportunistic navigation' systems, which can calculate a time and position from any nearby radio signals.

Mitigating the threat of interference with satellite systems and staying ahead of the attackers will require the same innovation and dedication we see in the field of cyber security. Ultimately, we need to see governments recognise secure navigation as a national security priority and dedicate the same effort and resources to this problem that it dedicates to cyber threats ●

Nigel Davies established and now leads QinetiQ's Secured Navigation group. The group has built an international reputation for high performance navigation solutions and for its security work on the European Galileo system.

The next generation of secure military satellite receivers

Picture credit: QinetiQ