# Te Matataua

The Scouting Party of Air Power

**RNZAF Air Power Development Centre Bulletin**

**Issue 22, July 2018**


# Spoofing and Jamming

## Reasons why Global Navigation Receivers can lie, or die

In June 2016, Moscovites in Russia began to complain that devices using Global Navigation Satellite Systems (GNSS), such as American GPS and Russian GLONASS, would sometimes show erroneous locations whenever driving or walking near the Kremlin. In many instances, the devices would place their location as at Vnukovo airport - 25 miles away from where they actually were. Taxis ordered by GPS-based apps such as Uber were sent to the wrong address and Pokemon would suddenly vanish as Pokemon Go players were seemingly teleported miles away.

One year later, the master of a ship near the Black Sea port of Novorossiysk noticed his GPS indicating that the vessel was 32 kilometres inland, at Gelendzhik airport. When he contacted other ships nearby, the master discovered that at least 20 others were similarly affected. While unconfirmed, the belief is that the Moscow and Black Sea events demonstrate that the Russians have developed a GNSS spoofing capability that can severely disrupt and confuse the geolocation abilities of GNSS users.


The military advantages associated with the ability to supplant good GNSS satellite data with false signals is significant. Defensively, spoofing can protect ones forces from kinetic attack by redirecting precision weapons that use global satellite systems for targeting guidance. It can also mislead ISR platforms, such as drones, away from areas of interest, enabling military activity to go unnoticed. Offensively, spoofing can paralyse the operational ability of opponents through the loss of vital position, navigation and timing (PNT) data; data that enables navigation for foot soldiers, land vehicles, ships and aircraft; search and rescue; and timing for communications and command and control. While reliance on GNSS data for operations is not total, in some military communities it is very close to being so. The US Army for instance has over 250,000 GPS-dependant systems, the loss or corruption of which, according to the US Army Asymmetric Warfare Group, "can be disastrous to an operation."

Disrupting GNSS signals is nothing new as jamming capability has been prevalent for many years. Surveillance drones were "jammed into virtual blindness" by Russian troops during Organisation for Security and Cooperation in Europe (OSCE) monitoring missions in 2014/15. A loss of GPS coverage in Norway last year during the largest Russian military exercises in years is believed to have been a not-so-subtle demonstration of capability, while GPS jamming in the current Syria conflict has contributed to that

theatre being described by the General in charge of US special operations activities as 'the most aggressive Electronic Warfare (EW) environment on the planet by our adversaries". Domestically the Russians are believed to have more than a quarter of a million cell towers equipped with GPS jamming devices as additional defence against precision weapons such as missiles.

North Korea allegedly subjected South Korean ships and aircraft to repeated jamming between 2010 and 2013, and has developed indigenous jammers by reverse-engineering Russian systems. Intelligence reports indicate that China has been conducting tests with vehicle-mounted GPS-jamming systems during exercises. The Americans have also subtly demonstrated GPS jamming capability. In 2016 and again earlier this year, the US Federal Aviation Authority issued regional warnings to aircrew that GPS-related navigation systems could be disrupted over the period of large military exercises which were occurring in the vicinity of the warning.

GNSS Jamming and spoofing are elements of what is termed Navigation Warfare (NAVWAR). Defined by NATO as "actions and/or technical means to assure position, navigation and timing information superiority", NAVWAR is a form of warfare that can be highly effective whilst also retaining an element of deniability, particularly during times of peace. In this respect, NAVWAR is similar to cyber-warfare. Overt NAVWAR capabilities are also being developed. For instance, in October 2017, the US Navy stated that it was going to pay Northrop Grumman nearly $8.9 million to create and fit a navigation warfare system into some of its E-2D Hawkeye airborne early warning and control (AEW&C) aircraft.

The ability to disrupt GNSS signals is relatively easy. Satellite signals are typically very weak – about 20 watts originating from 20,000 miles away. A one-watt transmitter in the vicinity of the receiver can easily override this signal. Jamming of signals is usually obvious, whereas spoofing can be more insidious. As the former president of the UK's Royal Institute of Navigation describes: "jamming just causes the receiver to die, spoofing causes the receiver to lie." A test by US scientists in 2012 fooled a drone into thinking its altitude was increasing, whereupon it then descended rapidly in its attempt to remain level. In 2013, they steered an $80 million yacht off course through GPS-spoofing.

Jamming or spoofing is not necessarily all-powerful. Many weapons and vehicles that rely on precision guidance also have complementary or alternate systems that enable continued guidance should GNSS signals be lost. For instance, the most common guided bomb used by the USAF, JDAM (Joint Direct Attack Munition), employs both GPS and INS (Inertial Navigation System – a system that uses internal accelerometers and gyroscopes) information for navigation. Should GPS be lost, INS takes over, though the accuracy of the bomb will be substantially degraded. Should GPS telemetry suddenly 'jump' miles away, as can be the case in spoofing, navigation systems may 'vote out' GPS information entirely, defaulting instead to backup systems such as INS. Slow, incremental corruption of GNSS data may not be recognised by on-board equipment however.

Encrypted GNSS systems are far more difficult to spoof than unencrypted systems and advances in GNSS receivers and antenna arrays have included complex algorithms for detecting and ignoring spoof signals. The systems most at risk of spoofing are legacy commercial-grade devices, but every system should be considered spoof-able due to continual advances in adversary capability. Many military forces now regularly practice operations within GPS-denied environments, exercising proven methods such as paper map and compass for navigation. Having a Plan B for whenever technology becomes unavailable or fails, is becoming ever more important.

**Key Points**

- GNSS signals are able to be jammed or spoofed.
- NAVWAR is a significant form of warfare that can influence the outcome of an operation or campaign.
- Total reliance on GNSS for navigation guidance is unwise. A 'Plan B' for GNSS-denied environments should always be considered.

## *APDC Update*

*The Journal of the RNZAF, 2018 has been released. Hardcopies have been sent to bases and camps and e-copies can be accessed on the APDC intranet and internet websites.*



E-mail: ohapdc@nzdf.mil.nz