How can shipowners protect against GPS jamming and spoofing?

Tue 15 May 2018 by Martyn Wingrove

GPS jamming and spoofing would be simple for those intent on disrupting a vessel and can have major consequences if mariners do not realise this is affecting vessel bridge electronics.

Information from the constellation of global positioning satellites feeds into multiple onboard electronics, such as ECDIS. Jamming can prevent that data from providing vital positioning information into navigation electronics, while spoofing can supply the wrong information.

Ultimately, this could lead seafarers to sail a ship in the wrong direction – perhaps leading to a collision or grounding, risking seafarer lives and pollution.

According to Totem Plus and DNV GL, jamming can be done by a simple jammer, transmitting on the same frequency and prohibiting the genuine GPS signal from being received and processed.

GPS spoofing requires more advanced equipment, capable of ‘cheating’ the GPS by sending dedicated signals that the GPS will interpret as genuine and consequently will show a wrong position.

Shipowners that are worried about GPS jamming and spoofing can train seafarers to recognise when bridge electronics, such as ECDIS, are either losing their GPS signal or receiving the incorrect data.

Colleges, such as Warsash Maritime Academy which provide ECDIS training, simulate these scenarios in courses for bridge officers.

Another solution is to install a device that protects bridge electronics from GPS jamming. This is an add-on to GPS that connects to the antenna and uses radio frequency algorithms to recognise when GPS is being jammed or spoofed.

GPS jamming and spoofing will be discussed at Riviera Maritime Media’s European Maritime Cyber Risk Management Summit, which will be held in association with Norton Rose Fulbright in London on 15 June.