



ON THE TRAIL OF THE GHOST SHIPS

AIS is vital for insurance purposes at the very least

Timothy Compston discovers that more and more ships are turning off their AIS (Automatic Identification System) or even switching their identities completely to sail under the security radar.

When employed properly AIS (Automatic Identification System), which provides a unique identification for each vessel as well as its position, course and speed, is invaluable from a safety and operational perspective as part of collision avoidance and traffic monitoring. Of course, no system is fool-proof and, unfortunately, a growing number of ships are making waves by circumventing AIS to disguise their nefarious activities, raising real security concerns as they change identity or

simply disappear.

The reasons why ships may decide to stop their AIS transmitting – or attempt to alter the associated data – so distorting the maritime picture, are many and varied. In some cases, the ship owners may be trying to break economic sanctions, while others are engaged in illegal fishing, people or drug smuggling, carrying arms shipments or even in extreme cases assisting terrorists. Tracking down the culprits is certainly no easy task especially when they cross thousands of miles of ocean and sail in and out of multiple ports and territorial waters. Just as those trying to hide their true

intent are becoming more sophisticated, so too has the technology to pick them out from all the noise and misdirection with maritime analytical techniques, when applied to AIS data gathered by satellites starting to make real headway too.

Interestingly, it was Israeli maritime analytics specialist Windward that first brought many of the issues around the misuse of AIS to the forefront thanks to a thought-provoking report published back in 2014 entitled: *AIS Data on the High Seas - An Analysis of the Magnitude and Implications of Growing Data Manipulation at Sea*. This research, which generated many headlines at the time, certainly didn't pull its punches concluding that AIS data – which up to that point was "widely perceived as a reliable source of information on ship activity worldwide" – had "critical vulnerabilities".

Looking in more detail at Windward's findings, which were based on aggregated shipping data and AIS-fitted vessels worldwide – estimated at over 200,000 vessels – the top five tactics giving cause for concern ranged from identity fraud and obscuring destinations to 'going dark', GPS manipulation and AIS spoofing. Considering these in turn, on the identity fraud front Windward discovered that ships were increasingly transmitting false or stolen identifying marks by taking

THE ABILITY OF SOMALI PIRATES TO TRACK A SPECIFIC VESSEL USING AIS IS A LATENT ONE

advantage of the AIS 'honours system' as ships are required to transmit their information, although there is still no way to validate the data. To put this into context, it was found that one percent of ships had used fake identification information – the IMO number – during the period of the research, which was very concerning given the overall numbers involved. For the next area, obscuring destinations, the final port of call was reported by ships on average only 41 percent of the time.

Another common manipulation practice flagged up by Windward was ships turning off their AIS transmissions completely, in fact it was discovered that over 25 percent of vessels across the globe are turning off their AIS at least 10 percent of the time. An added problem with AIS transmitters raised by the research was that they do not provide GPS validation. What this means in practice is that whatever positioning data is fed into the device is transmitted as the vessel's position regardless of where it is. From the middle of 2013 to the middle of 2014, a 59 percent increase in GPS manipulation was uncovered. The final aspect brought out in the study was so-called 'GPS spoofing' – something that had been investigated previously by a team at Trend Micro – and is basically the potential for people to create ghost ships where none exist.

Fast forward to today and new data provided exclusively to *intersec* by Windward, concerns activities off UK shores for April to May 2017 and shows that 59 vessels with invalid IMO numbers made a port call here, in addition four vessels deliberately turned off their transmissions within 10 days of a

port call. Beyond this, given the ongoing security concerns in the wake of the Manchester bomb attack, 10 ships stopped in Libyan waters and then up to two weeks later entered our waters (see image overleaf).

Omer Primar, product manager at Windward, is keen to reiterate the issues around AIS and the practical challenges of piecing together the pieces of the puzzle when certain ships try to undermine the system. He gives the analogy of someone switching off their phone or taking out the SIM card: "It is not that I am actually disappearing, I am simply eliminating a proxy of myself, which can help other people know where I am". In terms of AIS when it is turned off, he reckons that some countries like the UK may have the resources to keep a watchful eye on vessels through other measures, however the question arises as to what happens when the ship in question is further afield where there may not be the same capabilities: "I have no way of knowing what a ship is doing and pretty much the only source of knowing this is AIS. Turning off the AIS or manipulating it while at first it may seem very negligible for security, it actually has great ramifications if they want to hide where they are going or have come from," says Primar.

THE GREAT SWITCH OFF

Primar reckons that turning off an AIS transmission is not interesting in and of itself it is rather the interests which are dictating the behaviour of that vessel, the owners and the crew: "Imagine that I am trying to track someone using a cellphone and every time they went into a building it was turned off for three hours and then turned back on. What does that tell us? You don't know what he was doing for that time from that specific source. By itself, it is just an indication that something has happened. We need to have persistent surveillance, persistent tracking, to be able to hold the entity and then those small deviations and indications of potential risk, of potential interest, start popping up. That is the critical challenge because of how AIS is and that is a major part of what our [maritime analytics] technology is designed to do to deduce the first turning off (of AIS) and the conclusion". Primar says that Windward's ability to join the dots has been evolving over the past seven years and that the company's analytics solution reached its current level of maturity in late 2014, which coincided with the publication of the *AIS Data on the High Seas* report.

In terms of why vessels may manipulate AIS data, the examples offered up by Primar are wide ranging, whether it be a tanker whose owner is bankrupt, and there is an arrest warrant on the ship, so the vessel's identity is changed – to a different name and IMO number – every time it enters a certain country's waters, to boats fishing illegally seeking to hide their identities. Other reasons for going under the radar, according to Primar, include: tankers shipping oil as part of 'sanction busting', the smuggling of drugs, cigarettes, people and weapons, and, most concerning, to support terrorist activities. To add to this complicated equation, Primar underlines the fact that, to his knowledge, there is little enforcement going on with regards to AIS: "If a vessel is caught now manipulating its identity no one has jurisdiction

to do much about it. Maybe the only stick could be the insurance company because your insurance is void during the time when you have turned off your transmission," he concludes.

Turning to Gerry Northwood OBE, chief operating officer of MAST – a maritime risk management company – and former Royal Navy counter-piracy commander, he explains that although AIS started with relatively large ships it has gradually come down with regards to tonnage requirements to cover much smaller vessels. Addressing the case for AIS, Northwood draws a comparison with the aviation world: "Pretty much every aircraft that flies around the world files a flight plan yet you have got thousands of ships

AIS PROVIDES A UNIQUE IDENTIFICATION FOR EACH VESSEL AS WELL AS ITS POSITION AND COURSE

moving around internationally and in some ways, from an accountability point of view, they are more important than aircraft. The volume of goods that they are moving around is much greater and yet you don't have to file a voyage plan". For Northwood, given this information deficit, there is an important accountability side to AIS: "With AIS we can see what ships are doing and then that, of course, has been put into place by organisations like the IMO [International Maritime Organisation]". He also flags up the safety angle, which is a key driver here: "AIS transmits important course and speed and navigation information," says Northwood. Touching on the question of security where MAST's expertise lies, he goes on to explain when it makes

sense to activate a ship's AIS: "In the Indian Ocean, for example, best management practice advises that while ships are in the Gulf of Aden they keep their AIS on because there are warships there and they need to identify the ships that are going up and down the IRTC [Internationally Recommended Transit Corridor]".

LEGITIMATE REASONS TO TURN OFF

Northwood reveals that in certain cases there are, of course, legitimate security reasons for turning AIS off: "Outside the Gulf of Aden – in the wider reaches of the Indian Ocean – where you may not have warship protection so readily available, the BMP advice is that you may consider turning your AIS off". Expanding on his theme, Northwood puts the decision to stop using AIS in the context of who is looking at the data: "If you draw the conclusion that the Somali pirates are just as capable of owing an iPad and downloading an app to look at AIS and of course they have sat phones so they can phone through information to the vessels that they have at sea". Northwood admits that the ability of the Somalis to track a specific vessel or types of vessels is a latent one: "We haven't seen very much evidence of it to be honest. I think that they are more haphazard in the way they target their victims, but it is a possibility so turning off AIS for security reasons is there within best management practice".

Moving ahead, despite the issues AIS still has a key role to play for maritime safety. The latest guidance from the IMO on AIS – Resolution A.1106 (29) – acknowledges this by stressing that AIS should always be in operation when ships are underway or at anchor, unless the master believes that continual operation might compromise the safety and/or the security of the ship. It must be hoped that greater efforts will now be taken to crack down on those who are manipulating this data to hide their activities, unless they have a valid security reason for doing so ●

Timothy Compston

is a journalist and PR professional who specialises in security issues. He studied International Relations and Strategic Studies at Lancaster University, is PR director at Compston PR and a previous chairman of both the National Committee and CCTV PR Committee of the British Security Industry Association.

Libya Movements April to May 2017, provided by Windward UK



Picture credit: Windward UK