How sole reliance on AIS data could undermine your organisation's gBMP

In order to mitigate the risk of money laundering and terrorist financing, and avoid the likely criminal, reputational, and commercial damage that would occur as a result of non-compliance, organisations with exposures to shipping (including ship finance, trade finance, commodity trading, chartering and insurance services) are investigating the use of ship tracking services as a part of their overall risk management strategy. Knowledge of a ship's previous, current, and future trading patterns is required in order to achieve demonstrable best efforts, and is the foundation of any geospatial Best Management Practice (gBMP) programme.

For those considering ship tracking services, you may have found that the range of commercial solutions available on the market appear to be limited to Automatic Identification System (AIS)-based services. AIS-only ship tracking services may offer an adequate source of information for basic ship tracking. However, if you are evaluating these services for compliance purposes, it is crucial to understand the vulnerabilities of AIS and be aware of alternative, more secure and comprehensive risk management solutions such as those commonly utilised by governments and major shipping companies.

A recent critical report by Trend Micro (an independent internet content security and threat management consultancy) has drawn the attentions of the maritime and mainstream press to the vulnerabilities of AIS, in particular the security of the data and its susceptibility to hacking.

In this bulletin, we explore the vulnerabilities of AIS and suggest how PurpleTRAC (a new risk management and sanction compliance solution from Pole Star) can help underpin your implementation of gBMP.

Vulnerabilities of AIS

AIS has several major vulnerabilities, including:

AIS message transmission is not secure and can be falsified

Trend Micro has drawn attention to "vulnerabilities that allow an attacker to tamper with valid AIS data and inject invalid AIS data".[1] During experiments, Trend Micro's researchers proved that they were able to "hijack communications of existing vessels, create fake vessels, trigger false SOS or collision alerts and even permanently disable AIS tracking on any vessel".[2] According to Lloyds List, Trend Micro has highlighted "how easy it is to hack into the system that tracks the location of the world fleet".[3] AIS can be spoofed because it uses open standards (ITU M.1371 / NMEA0183) that can be obtained by anyone and used to decode the data.

Real world example: Ramtin

It was recently reported that the Iranian crude oil tanker Ramtin, which is managed and owned by Tabuk Maritime (a company sanctioned by OFAC), had hacked its own AIS to disguise its activities near Singapore.[4]

AIS equipment is not required to be continuously switched on

AIS messages are transmitted using very high frequency (VHF) radio waves and received, without restriction, by anyone with an AIS receiver (who can then publish the data on the web and/or use the data for illegitimate purposes). Consequently, there are legitimate operational concerns that pirates and/or criminals could use this information to locate and target specific ships and cargoes. To counter this, the International Maritime Organization (IMO) issued regulatory guidance to ships masters that, if the ship was considered to be under threat, its AIS could be switched off. This does happen when ships transit high-risk areas where there is an obvious threat of piracy, when ships with high-interest cargo wish to avoid commercial detection, and when ships conducting illegal ship-to-ship transhipments attempt to conceal their activities.[5]

AIS was not designed to be a global tracking system

AIS is recognised by the IMO for the purpose of collision avoidance and not as a global ship tracking system. Furthermore, when the IMO introduced ship tracking as an international security requirement (with the introduction of the Long-Range Identification and Tracking (LRIT) regulation) it specifically excluded the use of AIS due to its inherent insecurity, and employed the more secure, robust, and reliable Inmarsat-C technology instead.

Satellite-AIS has message collection and latency limitations

In high-density shipping areas where thousands of ships may be transmitting AIS messages, it is a challenge for S-AIS systems to efficiently collect, process, and download all of the messages. The result of this is that many messages are lost due to data collisions. Research indicates that typical S-AIS receivers are able to receive less than 50% of messages in medium to high-density areas. The S-AIS provider then has to clean (or "de-collide") the data in order to extract useful information from it. This data processing exercise adds a delay (known as "latency") to the delivery of the message.

[1, 2] Vulnerabilities Discovered in Global Vessel tracking Systems, Trend Micro, 15 October 2013, http://blog.trendmicro.com/trendlabs-security-intelligence/vulnerabilities-discovered-in-global-vessel-tracking-systems

[3] AIS can no longer be trusted, says hacking expert, Lloyds List, 18 October 2013

[4] Iranian Tanker Hacks AIS to Disguise Itself Off Singapore, gCaptain, 25 October, 2013, http://gcaptain.com/iranian-tanker-hacks-disguise/

[5] Phantom Ships Expose Weakness in AIS Vessel-Tracking System, Bloomberg, 29 October 2013, http://www.bloomberg.com/news/2013-10-29/phantom-ships-expose-weakness-in-vessel-tracking-system-freight.html

How AIS works

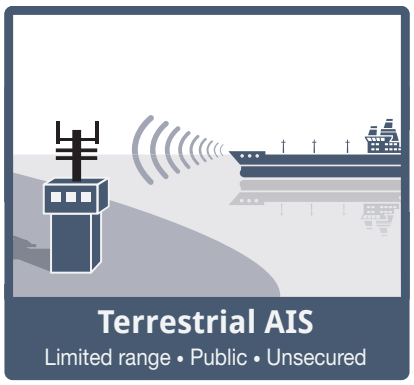
The Automatic Identification System (AIS) is a VHF (very high frequency) radio tracking system that is used by ships and vessel traffic services to identify and locate other nearby ships for the primary purpose of collision avoidance.

The AIS regulation requires equipment to be fitted aboard all ships of 300 gross tonnage and upwards engaged on international voyages, cargo ships of 500 gross tonnage and upwards not engaged on international voyages, and all passenger ships irrespective of size. The requirement became effective for all ships 31 December 2004. The regulation requires that AIS shall:

- **Provide information (including the ship's identity, type, position, course, speed, navigational status and other safety-related information) automatically to appropriately equipped shore stations, other ships and aircraft**
- **Receive the above information automatically from other AIS enabled ships**
- **Monitor and track ships**
- **Exchange data with shore-based facilities**

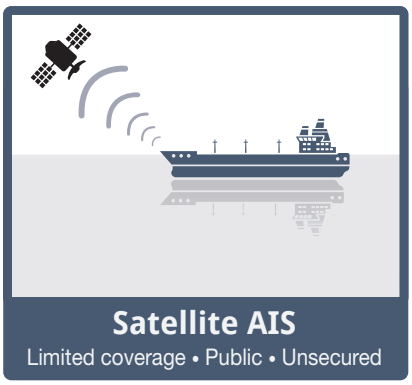
Terrestrial (T-AIS)

The AIS equipment aboard a ship broadcasts messages to AIS receivers on other ships and ashore (typically ports). Such T-AIS equipment can detect messages from up to 50 nautical miles and therefore provides effective ship-to-ship and coastal coverage.



Satellite AIS (S-AIS)

S-AIS systems use a network of satellite-based receivers to detect and collect AIS messages transmitted from ships. S-AIS is effective for basic and historical ship tracking. However, the system does have message collection and latency limitations in respect of near real-time tracking.



Achieving demonstrable best efforts

Avoiding sanctioned countries, either directly or by indemnification, is not sufficient. Organisations with exposures to shipping risk are expected to know if any business relationships are linked to such countries. By definition, this includes the physical asset (the ship) and related group beneficial owner, registered owner, operator, manager, and technical manager, and extends to the ship's chartering, cargo, cargo financing, and associated insurances including hull, P&I, cargo, war risk, and K&R.

The solution: PurpleTRAC

PurpleTRAC is a geopolitical risk management and economic sanctions compliance solution designed by and for organisations with exposures to shipping risks. Delivered as a Software-as-a-Service (SaaS) hosted application to registered users on a subscription-only basis, PurpleTRAC consists of three integrated processes: ship screening, ship tracking and archiving & reporting.

Screening

Screening consists of a series of automatic checks to provide critical and advisory information regarding a selected ship's current and past exposure to risk.

- **Global Sanctions:** screens the ship and its associated group beneficial owner, registered owner, operator, ship manager, and technical manager against a comprehensive range of 37 international sanctions lists[8], and generates an alert if a positive match is returned.
- **Flag State, Class Society, and Ship Quality Performance:** screens the ship against a range of flag, class, and Port State Control (PSC) inspection deficiency and detention databases[9] and blacklisted ports and generates an alert if a positive PSC match is returned.
- **Ship Movement History:** screens the ship against OFAC sanctioned countries and US Port Security Advisory bulletin ports listings using the last 90-days of available Automatic Identification System (AIS) position data and generates an alert if a positive match is returned.

A comprehensive Screening Report is available on the user interface, via download and by email.

Tracking

PurpleTRAC actively tracks ships on a continuous or voyage-based basis.

- **Hybrid Track technology:** combines data from multiple satellite tracking services (including the ship's secure Inmarsat-C terminal and its AIS equipment) into a single coherent position track (whilst managing minor inconsistencies and reporting major anomalies).
- **Detection & alerts:** actively monitors the ship's movements for key pre-defined events (e.g. approach or entry to high-risk areas[10]).
- **Daily screening:** daily screening against the full range of global economic sanctions lists.

A Management Report is available on the user interface, via download and by email.

Archiving & Reporting

PurpleTRAC maintains an up-to-date record of all users' historical and on-going activities, providing a tamper-resistant, auditable and verifiable statement of your organisation's geopolitical risk management and sanctions compliance activity.

A Trade Report is available on the user interface, via download and by email.

Find out more about PurpleTRAC at http://purpletrac.polestarglobal.com

[8] Data supplied by Dow Jones Risk & Compliance
[9] Data supplied by IHS
[10] As defined by the London Joint War Committee