Lloyd's List Intelligence

Whitepaper

Tackling AIS spoofing with **Seasearcher Advanced Compliance**

What you need to know about the rise of AIS spoofing and how you can detect it using our comprehensive solution.

Why is AIS spoofing on the rise?

Automatic Identification System (AIS) spoofing is becoming more frequent as bad actors evolve and find new ways to circumvent and evade sanctions.

With geopolitical tensions at their highest since the Cold War and Europe experiencing its first war since the Yugoslav Wars, sanctions have become a key foreign policy tool used by multiple governments to influence behaviour.

In May 2020, the U.S. Departments of State, Treasury, and Coast Guard issued a Sanctions Advisory for the Maritime Industry, Energy, and Metal Sectors, and Related Communities. This advisory provided guidance to "address illicit shipping and sanctions evasion practices". Since then, other advisories and restrictions have followed, including from the United Kingdom's Office of Foreign Sanctions Implementation (OFSI) and the European Union (EU), as well as the multilateral Russia Oil Price Cap (OPC).

All these advisories emphasise a common point: deceptive shipping practices (DSPs) pose significant challenges to maritime safety, security, and compliance enforcement. Among these DSPs, AIS spoofing is particularly insidious. AIS spoofing involves a vessel deliberately transmitting false positional data to appear in a different location than its actual position. Detecting this requires advanced tracking technologies and machine learning (ML) solutions.

Historically, AIS spoofing has been used to conceal illicit activities, especially during warfare and, more recently, for evading sanctions at Venezuelan and Iranian ports.

However, since Russia's war in Ukraine began, the use of AIS spoofing has increased significantly.

According to Lloyd's List Intelligence (LLI) , AIS spoofing instances increased by over 50% from 2022 to 2023. Even before the war, Russia demonstrated its expertise in AIS manipulation by spoofing the British warship HMS Defender's route through the Russian naval base of Sevastopol in 2021, even though the vessel was transiting Ukrainian waters.

During the conflict and subsequent sanctions on its oil trade by Western nations, Russian vessels have increasingly used AIS spoofing to hide activities related to crude and petroleum product exports and grain shipments from seized Ukrainian territories. This includes masking vessel locations while entering high-risk ports to collect sanctioned cargo or engage in ship-to-ship transfers. For example, in late 2022, LLI identified multiple tankers picking up apparent Venezuelan oil products while spoofing their locations to appear off the coast of Angola, even though our proprietary terrestrial AIS network confirmed that the vessels were actually in Venezuela.

The importance of advanced vessel-tracking systems

In an April 2023 alert, the U.S. Office of Foreign Assets Control (OFAC) raised further concerns about AIS spoofing, specifically highlighting its potential role in evading the OPC.

The alert noted instances where tankers, possibly manipulating their AIS, were involved in the export of Eastern Siberia-Pacific Ocean oil pipeline crude from Pacific Russian ports such as Kozmino. This manipulation was particularly prevalent as oil prices exceeded the $60 per barrel cap.

OFAC representatives also emphasised the importance of advanced vessel tracking services in detecting spoofing.

> "What we've seen is that sometimes there will be a discrepancy between what a very basic vessel-tracking service shows and a more sophisticated vessel-tracking service will show."
>
> **Claire McCleskey**
> Assistant director of sanctions compliance and evaluation at OFAC

"The very basic vessel-tracking platforms will show that a ship was somewhere in the area around Kozmino for example, but will show very clearly that they did not go anywhere near it, and then when you access a more sophisticated vessel-tracking system, you can see clearly that ship did in fact, call at Kozmino."

Seasearcher Advanced Compliance, the flagship solution from LLI, belongs in the latter category. Our spoofing detection dynamically leverages Machine Learning models and proprietary terrestrial AIS networks to accurately identify spoofed vessel locations. This white paper will demonstrate exactly how it works.

How does Seasearcher Advanced Compliance detect AIS spoofing?

It's important to note that GPS jamming and AIS spoofing are not the same thing. GPS jamming, also known as Global Navigation Satellite System (GNSS) jamming, has been a common tactic used by governments and organisations to disrupt radio frequency detection.

This occurs when external interference disrupts GNSS signals, causing multiple vessels in a specific area to falsely appear in one location while actually being elsewhere. This interference, often observed in areas like the Kerch Strait in the Black Sea, can manifest as straight-line coordinates or random patterns transmitted from vessels' AIS.

In this scenario, a third-party actor unrelated to the vessel – likely situated close to shore – broadcasts a GNSS signal containing false GPS coordinates. Vessels latch onto this signal, prioritising it over satellite signals directly above them. Consequently, the GPS coordinates are rebroadcasted as part of the AIS data package, resulting in the vessel appearing off-course or even on dry land. Notable locations affected include airports, city centres, and government buildings.

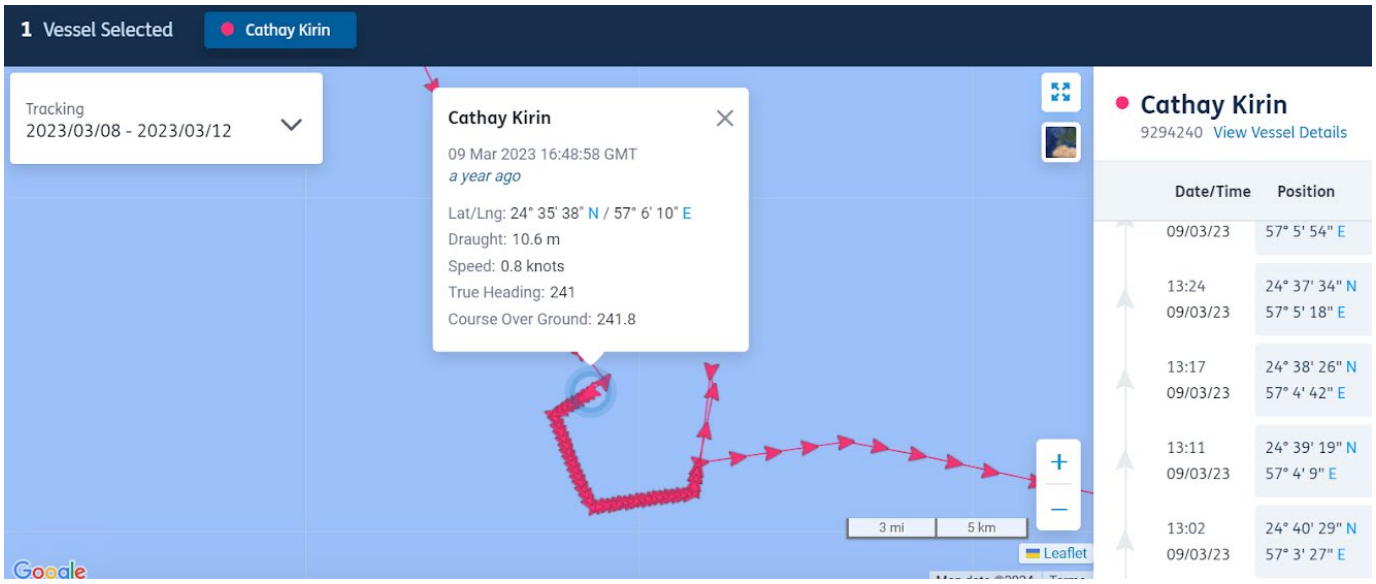
AIS spoofing, on the other hand, is a more sophisticated technique that's increasingly challenging to detect. Currently, the most effective method for detecting spoofing is a machine learning (ML) approach, as it can identify intricate anomalies within AIS messages.

Powerful jammers can override ships' signals, making them show up in the wrong places.

Source: Lloyd's List Intelligence / Seasearcher

Date/Time	Lat	Lng	AIS Destination	Heading	Speed over	Course over	Source Type	Distance (nm)	Distance (m)
09/03/2023 16:48	24.59395	57.10276	SOHAR ETA: 0	241	0.8	241.8	Satellite	0.18	325.25
09/03/2023 17:49	24.59235	57.10007	SOHAR ETA: 0	241	0.3	241.8	Satellite	0.18	327.35
09/03/2023 18:50	24.59076	57.09735	SOHAR ETA: 0	243	1	242.3	Terrestrial	0.17	321.80
09/03/2023 19:50	24.58923	57.09465	SOHAR ETA: 0	243	1	243.8	Terrestrial	0.17	323.16
09/03/2023 20:51	24.58772	57.09192	SOHAR ETA: 0	243	1	244.5	Terrestrial	0.18	325.32
09/03/2023 21:52	24.58624	57.08915	SOHAR ETA: 0	245	1.1	245.1	Terrestrial	0.17	323.50
09/03/2023 22:52	24.58482	57.08636	SOHAR ETA: 0	246	0.6	246.1	Satellite	0.15	275.55
09/03/2023 23:54	24.58302	57.0845	SOHAR ETA: 0	156	0.8	157.1	Satellite	0.20	361.35
09/03/2023 00:54	24.57997	57.08571	SOHAR ETA: 0	156	0.9	156.9	Terrestrial	0.22	400.60
09/03/2023 02:01	24.57659	57.08707	SOHAR ETA: 0	156	0.9	156.1	Terrestrial	0.20	366.92
09/03/2023 03:01	24.5735	57.08832	SOHAR ETA: 0	156	0.9	155.9	Terrestrial	0.19	360.95
09/03/2023 04:02	24.57046	57.08957	SOHAR ETA: 0	155	0.3	156.3	Terrestrial	0.20	362.36
09/03/2023 05:02	24.56742	57.09084	SOHAR ETA: 0	155	0.3	155.3	Terrestrial	0.19	360.30
09/03/2023 06:02	24.5644	57.09212	SOHAR ETA: 0	155	0.8	155.3	Terrestrial	0.20	361.61
09/03/2023 07:02	24.56137	57.09342	SOHAR ETA: 0	155	1.1	155.3	Terrestrial	0.19	360.68
09/03/2023 08:02	24.55836	57.09474	SOHAR ETA: 0	154	0.9	154.4	Terrestrial	0.20	370.52
09/03/2023 09:04	24.55528	57.09612	SOHAR ETA: 0	154	1.1	153.9	Terrestrial	0.19	359.82
09/03/2023 10:04	24.55229	57.09748	SOHAR ETA: 0	153	0.3	153	Terrestrial	0.19	360.62
09/03/2023 11:05	24.54931	57.09888	SOHAR ETA: 0	152	0.6	152.7	Terrestrial	0.20	361.65

These anomalies, such as fabricated GPS coordinates, can be identified by analysing the reported GPS positions (latitude and longitude) and speed over ground (SOG) against the calculated feasibility of distance, speed, and time.



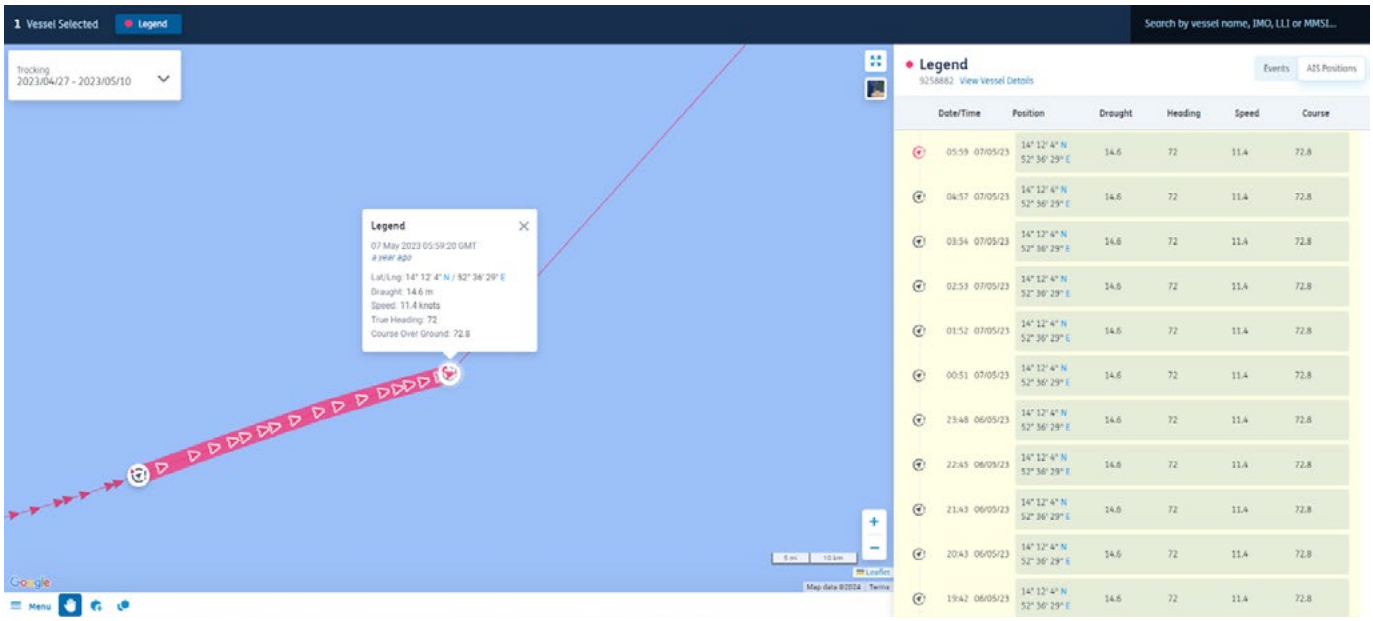
Cathay Kirin (IMO: 9294240) vessel's spoofing pattern in the Gulf of Oman

In this example, vessel Cathay Kirin (IMO: 9294240) is seen to be sailing off the coast of Sohar, Oman. However, upon closer examination of its AIS positions during this time, it is clear that something is off. The vessel appeared to be moving in
an unusual rectangular pattern, which doesn't align with traditional maritime behaviour.

When calculating the distance between these positions and considering the vessel's reported speed, math confirms that the vessel should have been moving much faster. This discrepancy persists for three days, during which the vessel maintains this irregular tracking pattern.

This is concerning because the vessel may be engaged in DSPs. For instance, it could have had enough time to travel to Iran and back while maintaining this deceptive tracking behaviour. Such actions could be aimed at circumventing sanctions or engaging in other illicit cargo activities.

Let's take a look at another example of the vessel Legend (IMO: 9258882). This vessel was travelling along the Gulf of Aden, reporting a speed of 11.2 knots. However, the GPS coordinates (latitude and longitude positions) showed the vessel as stationary from 4 to 7 May 2023.



Legend (IMO: 9258882) transiting along the Gulf of Aden displaying false AIS SOG messages

Seasearcher employs a comprehensive approach to detecting anomalies in vessel tracking. LLI leverages ML techniques to identify irregularities, and further validate these findings using the metadata from our proprietary terrestrial AIS network. This enables our platform to accurately determine the true location of vessels, contrasting with the locations they report.

For instance, a common occurrence we observe is when vessels spoof their positions along the coast of West Africa, making it appear as though they are loading cargo off the coast of Angola when in reality they are loading in Venezuela. Our proprietary terrestrial AIS network often detects these spoofed positions, providing us with valuable insights into the vessel's true whereabouts.

In most cases of AIS spoofing, the manipulation occurs on the AIS transceiver onboard the vessel. Our proprietary terrestrial AIS network plays a crucial role in determining the vessel's actual location during spoofing incidents. But we have also encountered a new pattern of spoofing where the AIS positions are manipulated after receiving the AIS message, posing additional challenges for detection.

Date/Time	Lat	Lng	AIS Destination	Heading	Speed over	Course over	Source Type
15:49:15 GMT 07/05/2023	14:20104	52.60813	SG SIN ETA	72	11.4	72.8	Satellite
15:23:36 GMT 07/05/2023	14:20104	52.60813	SG SIN ETA	72	11.4	72.8	Satellite
14:23:10 GMT 07/05/2023	14:20104	52.60813	SG SIN ETA	72	11.4	72.8	Satellite
13:16:11 GMT 07/05/2023	14:20104	52.60813	SG SIN ETA	72	11.4	72.8	Satellite
12:14:20 GMT 07/05/2023	14:20104	52.60813	SG SIN ETA	72	11.4	72.8	Satellite
11:!3:31 GMT 07/05/2023	14:20104	52.60813	SG SIN ETA	72	11.4	72.8	Satellite
10:06:50 GMT 07/05/2023	14:20104	52.60813	SG SIN ETA	72	11.4	72.8	Satellite
09:03:21 GMT 07/05/2023	14:20104	52.60813	SG SIN ETA	72	11.4	72.8	Satellite
08:02:49 GMT 07/05/2023	14:20104	52.60813	SG SIN ETA	72	11.4	72.8	Satellite
07:02:48 GMT 07/05/2023	14:20104	52.60813	SG SIN ETA	72	11.4	72.8	Satellite
05:59:20 GMT 07/05/2023	14:20104	52.60813	SG SIN ETA	72	11.4	72.8	Satellite
04:57:12 GMT 07/05/2023	14:20104	52.60813	SG SIN ETA	72	11.4	72.8	Satellite
03:54:00 GMT 07/05/2023	14:20104	52.60813	SG SIN ETA	72	11.4	72.8	Satellite
02:54:00 GMT 07/05/2023	14:20104	52.60813	SG SIN ETA	72	11.4	72.8	Satellite
01:52:15 GMT 07/05/2023	14:20104	52.60813	SG SIN ETA	72	11.4	72.8	Satellite
00:52:15 GMT 07/05/2023	14:20104	52.60813	SG SIN ETA	72	11.4	72.8	Satellite
23:48:16 GMT 07/05/2023	14:20104	52.60813	SG SIN ETA	72	11.4	72.8	Satellite

Unfortunately, the open-source nature of AIS communication makes it susceptible to manipulation at various points before the data reaches our servers.

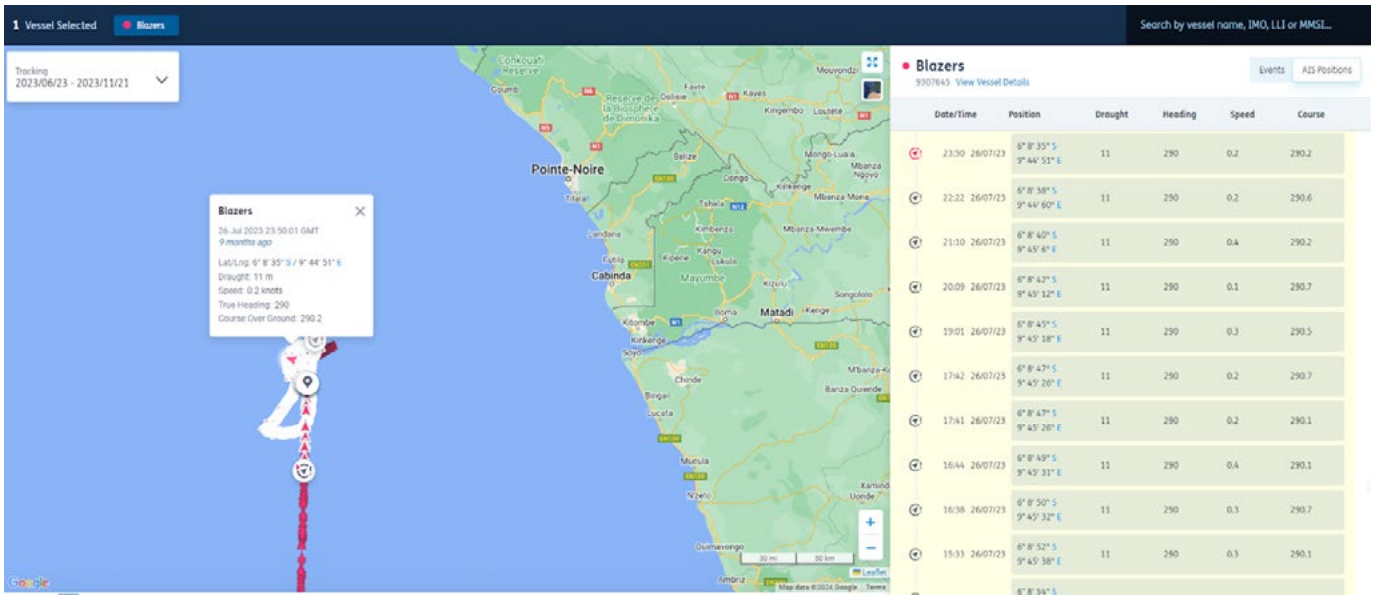
However, at LLI, we employ a multi-layered approach which enables us to effectively identify and counteract spoofing – both onboard the vessel and within the receiving network.

Detecting spoofing onboard the vessel

The simplest method to spoof an AIS transceiver is to simply have two of them onboard. This is a common tactic employed by vessel crews to deceive and manipulate their reported location.

They program identical static information such as Maritime Mobile Service Identity (MMSI), name, and IMO into both transceivers – then connect one of them to a GPS system projecting a false location, different from the vessel's actual position.

There are numerous examples of such spoofing cases, especially evident among ballast crude oil tankers anchored off the coast of Luanda, Angola, over the past two years. One notable example is the Blazers (IMO: 9307645), a 19-year-old crude oil tanker. Owned by Global Marine Limited, a Hong Kong-based company, the tanker has been navigating between the Far East, Singapore, and West Africa for the last year and a half.



Vessel Blazers (IMO: 9307645) loitering off the coast of Angola for 3 months whilst spoofing

In 2023, the vessel was observed exhibiting an unusual tracking pattern near the lower Congolese basin, indicating AIS spoofing. This suspicious behaviour was repeated three months later, raising further concerns about the vessel's integrity and compliance with regulations.

Further scrutiny revealed that this vessel was closer to Venezuela than it was to West Africa, as evidenced by the source of the AIS messages received for this vessel at that time.

As depicted in the table below, we can observe that the AIS positions for this vessel originated from AIS receivers located in ports in Grenada, Trinidad, Tobago, and Venezuela. This confirms that the empty crude oil tanker was indeed moving closer to Venezuela. Without access to the metadata of our proprietary AIS network, proving this would have been improbable.

message_ts	latitude	longitude	sog	cog	heading	station
2023-04-16 03:57:25	-5.835852	10.198048	0.2	290.2	290	st_georges
2023-04-16 03:58:05	-5.835845	10.198031	0.3	290.8	290	st_georges
2023-04-16 06:40:55	-5.834299	10.193804	0.2	290.5	290	point_fortin
2023-04-16 06:41:05	-5.834297	10.193799	0.1	290.8	290	point_fortin
2023-04-16 06:41:15	-5.834295	10.193795	0.3	290.6	290	point_fortin
2023-04-16 06:51:25	-5.834199	10.193531	0.1	290.7	290	point_fortin
2023-04-16 06:53:14	-5.834182	10.193485	0.2	290.8	290	point_fortin
2023-04-16 19:11:16	-5.827174	10.174326	0.4	290.7	290	puerto_la_cruz
2023-04-16 19:11:25	-5.827172	10.174323	0.1	290.7	290	puerto_la_cruz
2023-04-16 19:11:45	-5.827169	10.174315	0.2	290.7	290	puerto_la_cruz
2023-04-16 19:11:56	-5.827167	10.174309	0.4	290.8	290	puerto_la_cruz
2023-04-16 19:12:06	-5.827166	10.174304	0.2	290.6	290	puerto_la_cruz
2023-04-16 19:13:36	-5.82715	10.174266	0.4	290.6	290	puerto_la_cruz
2023-04-16 19:13:45	-5.827149	10.174263	0.1	290.6	290	puerto_la_cruz
2023-04-16 19:13:56	-5.827147	10.174258	0.4	290.3	290	puerto_la_cruz
2023-04-16 19:16:36	-5.827122	10.174188	0.4	290.6	290	puerto_la_cruz
2023-04-16 19:16:46	-5.82712	10.174184	0.2	290.1	290	puerto_la_cruz
2023-04-16 19:16:55	-5.827119	10.17418	0.3	290.1	290	puerto_la_cruz
2023-04-16 19:17:46	-5.82711	10.174158	0.2	290.7	290	puerto_la_cruz
2023-04-16 19:18:05	-5.827109	10.17415	0.1	290.8	290	puerto_la_cruz

Detecting spoofing within the receiving network

Spoofing the receiver involves a more intricate method, akin to hacking. In this scenario, a hacker or malicious actor gains unauthorised access to an AIS receiving station and generates a new set of AIS messages for a vessel using its unique MMSI.

These forged AIS messages often appear remarkably authentic, sometimes even replicating previous legitimate AIS tracking data of the vessel or another. Detecting such manipulations can be challenging, but employing an ML approach helps as it's highly improbable for the exact same set of AIS messages to occur more than once.

However, having knowledge of the geographical locations of AIS receiving stations provides a significant advantage in detecting this kind of spoofing. By monitoring the locations from which AIS messages originate, one can identify stations that might have been compromised.

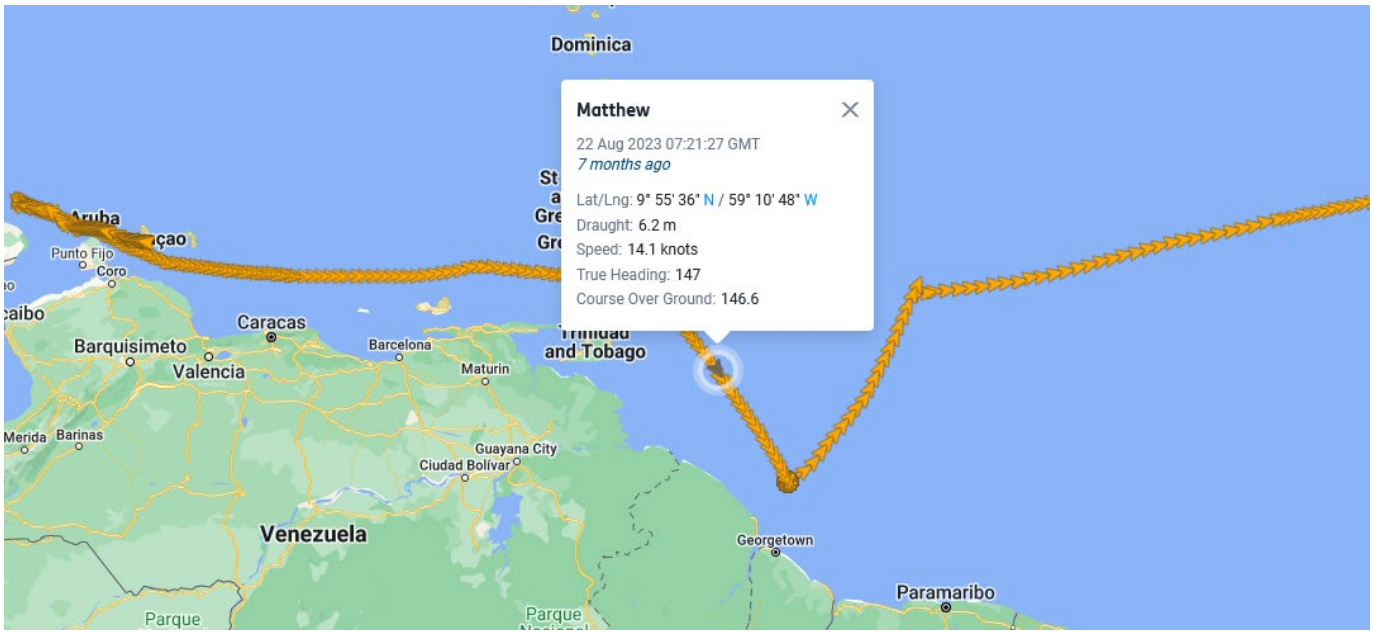
For instance, if an AIS receiving station reports messages for a vessel at a location that contradicts its known maritime movements, it indicates a potential hacking attempt.

The vulnerability of AIS systems to hacking has been a topic of concern for some time. In a 2014 paper titled, Threats at Sea: A Security Evaluation of AIS, cybersecurity firm Trend Micro discussed the possibility of 'AIS hijacking' where attackers could override genuine AIS messages with fabricated signals, typically targeting AIS receivers in ports. Unfortunately, this vulnerability extends to all AIS vessel tracking providers.

A notable case that exemplifies this vulnerability occurred with the vessel Matthew (IMO: 9228150), which came to our attention after being intercepted by the Irish Navy and was subsequently flagged by a prospective client. Upon reviewing the vessel's AIS data during its voyage past South America, anomalies were detected. Between August 19th and September 23rd, 2023, the vessel's AIS signals were received by our AIS receiving station in Dubai, United Arab Emirates.

Some telltale signs of this type of spoofing include circular movements recorded by the vessel's AIS, inconsistent with typical maritime behaviour, and AIS signals received by a station located over 3,000 nautical miles away from the vessel's reported location. Our hypothesis suggests that a group operating out of Dubai may be providing false AIS signals to the Dubai AIS receiver station, allowing the vessel to conduct covert activities by turning off its transponder.

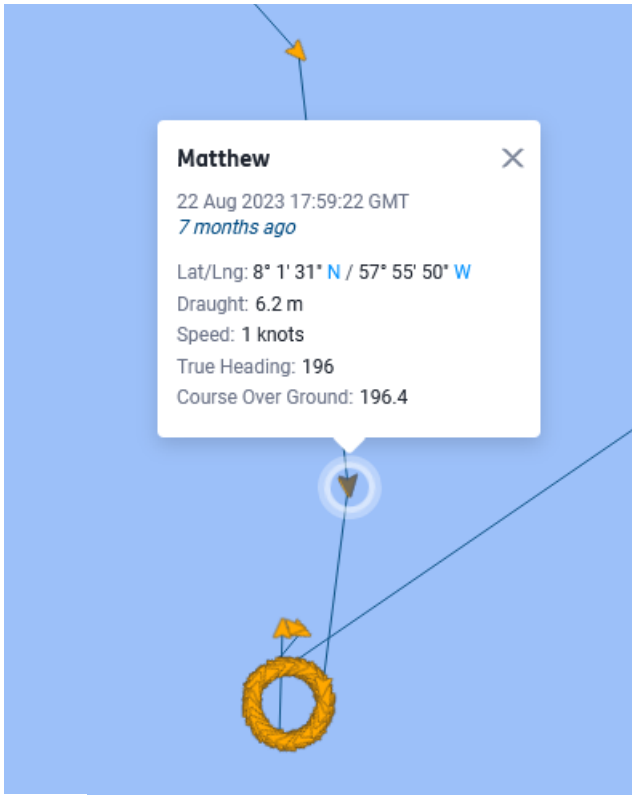
Supporting evidence includes the absence of AIS signals detected by any other station during the period of spoofing, despite vessels in the vicinity of Dubai typically being picked up by other local AIS stations, such as Abu Dhabi.



The Matthew vessel (IMO: 9228150) as it travelled to the coast of Guyana to conduct its spoofing activities.

This case is just one example among many. Unfortunately, such DSPs are likely to become more prevalent over time as bad actors seek to evade detection by technology providers like LLI. This trend raises important questions about the future of AIS and its effectiveness in ensuring compliance.

As an industry, we need to explore strategies to enhance the security or encryption of AIS technology or make alternative tracking sources more widely accessible. Finding viable solutions to these challenges will take time and careful consideration.



The circular behaviour depicted from the AIS data received from Matthew (all detected by the AIS receiver in Dubai).

Lloyd's List Intelligence

Combat AIS spoofing with Seasearcher Advanced Compliance

AIS spoofing is quickly becoming the primary method for companies and vessels to evade sanctions regulations. For this reason, relying on basic vessel-tracking systems that do not detect spoofing is no longer sufficient to ensure compliance.

Our comprehensive solution lets you:

- Leverage state-of-the-art machine learning to spot AIS spoofing patterns effectively
- Take immediate action upon detecting evidence of AIS spoofing, such as identifying the true position of the vessel through our proprietary AIS network
- Ensure efficient use of resources by confirming validated spoofing events and avoid wasting time on potential false positives
- View actionable insights into vessel movements and positions during suspected spoofing incidents
- Share your findings seamlessly with stakeholders across your organisation and your potential new customers with our in-built escalation features

When you use Seasearcher Advanced Compliance, you're better equipped to navigate the evolving threats of maritime security with confidence and efficiency.

Watch our demo > **Book a consultant >**

About Lloyd's List Intelligence

We are the industry experts delivering actionable maritime insight, data, and analytics trusted by 60,000 professionals to drive commercial advantage, evaluate risk, and support the efficient and lawful movement of seaborne trade. Our advanced analytics, artificial intelligence, and expertise transform unparalleled data into powerful insight through data services, news and commentary, and publications.

Customer success team

UK/US office:
+44 (0)20 7509 6499

Opening hours:
9am-5pm GMT

APAC office:
+65 6028 3988

Opening hours: 9am-6pm SGT (GMT+8)

UK office / Commerical sales

Lloyd's List Intelligence: +44 7741136029

Lloyd's List:
+44 (0)20 7017 5392

Regional sales

Asia Office:
+65 9027 3024

US Office:
+1 (917)843 6986

Learn more at lloydslistintelligence.com