ROKE

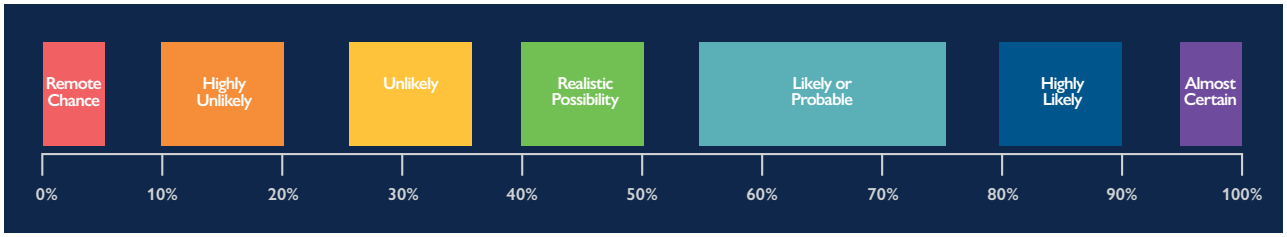
Spoofing and deceptive shipping

July 2024

The Roke Intelligence Advantage

The Probability Yardstick

Almost all intelligence assessments contain a degree of uncertainty. In order to avoid any misinterpretation, these intelligence assessments are categorised using the terms outlined in the image below, instead of using numerical probabilities. Throughout all Roke products the scale of probability is split into these seven categories. The use of this standard ensures analysts can make reliable judgments and avoid inappropriate use of terms.

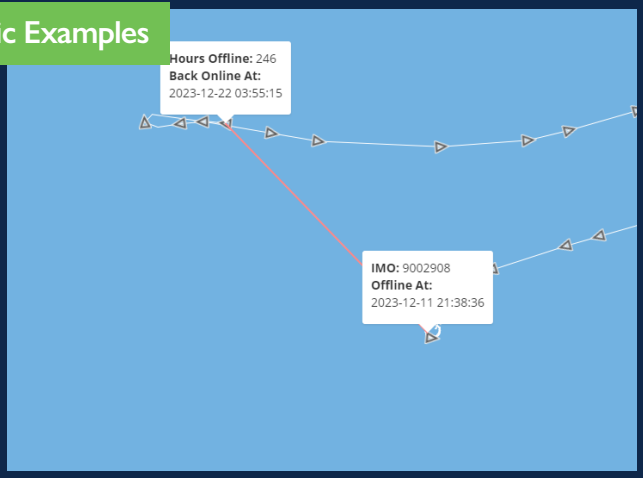


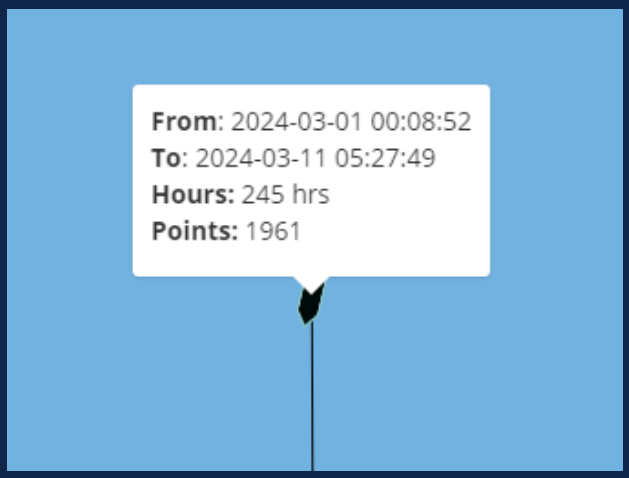
Spoofing Classification

Currently Roke classifies any GNSS manipulation (AIS spoofing) into four main categories: Basic, Transit, Anchor or Sophisticated. These are then broken down further into sub-categories with the aim to continue building a repository of further events and identifying characteristics that can bring insight into methodology and actors.

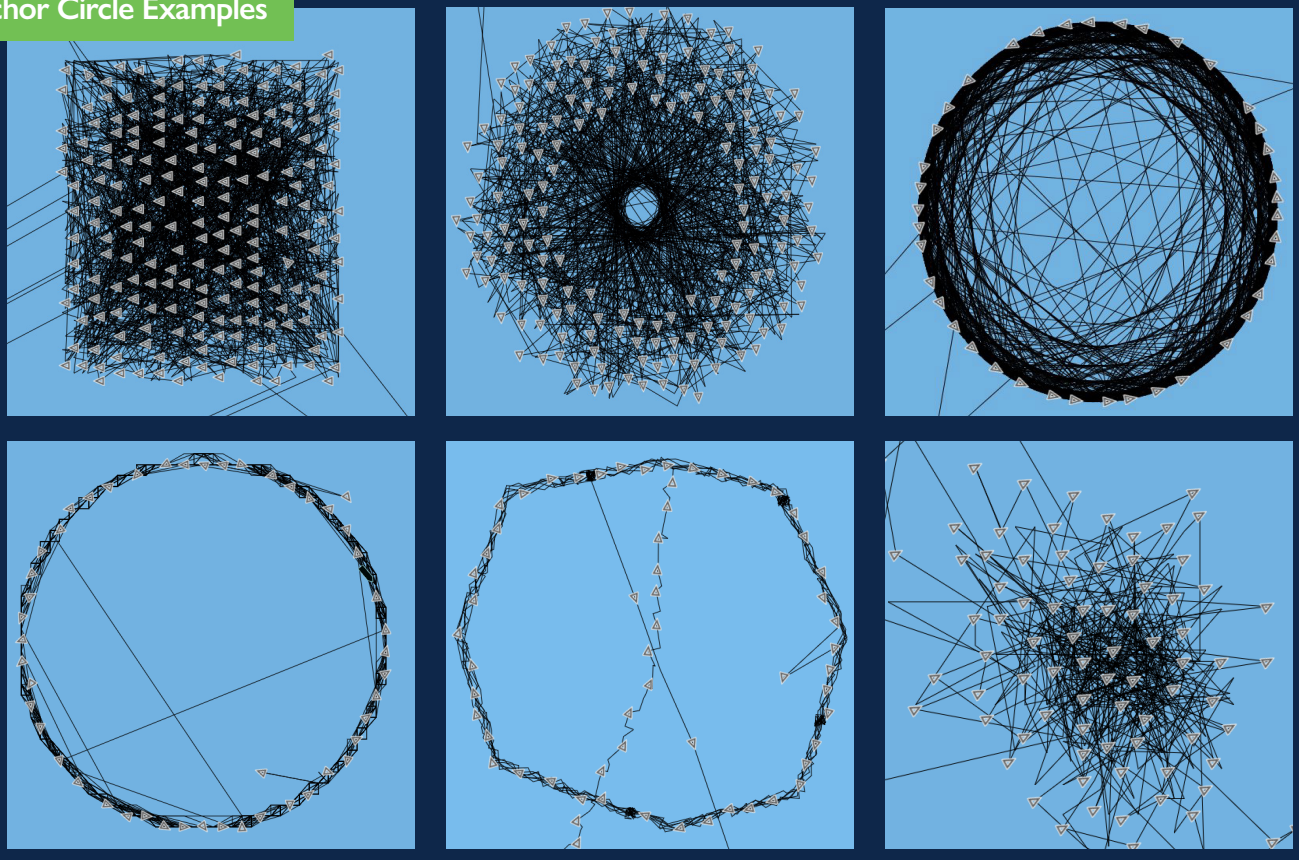
GNSS Manipulation

Basic Examples



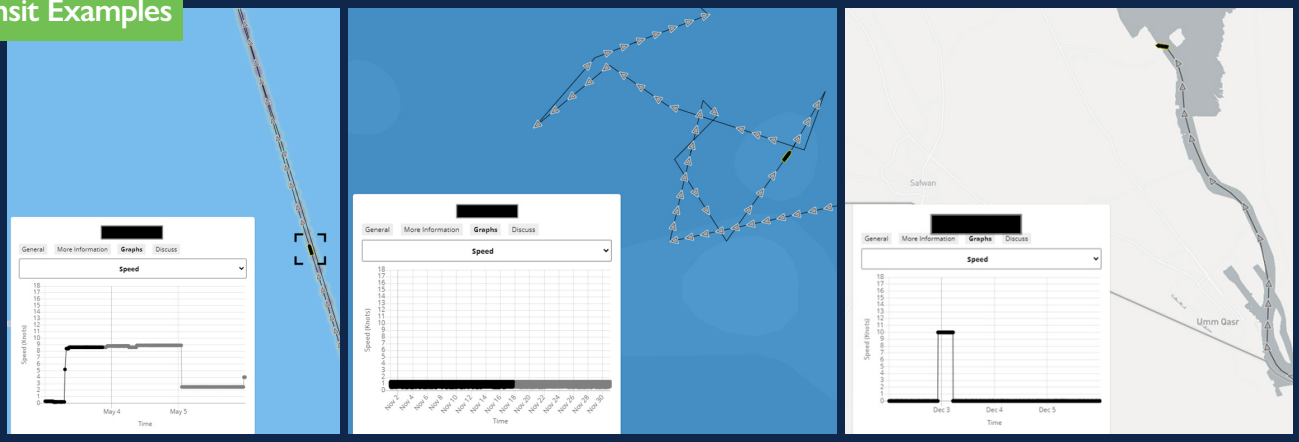


Anchor Circle Examples

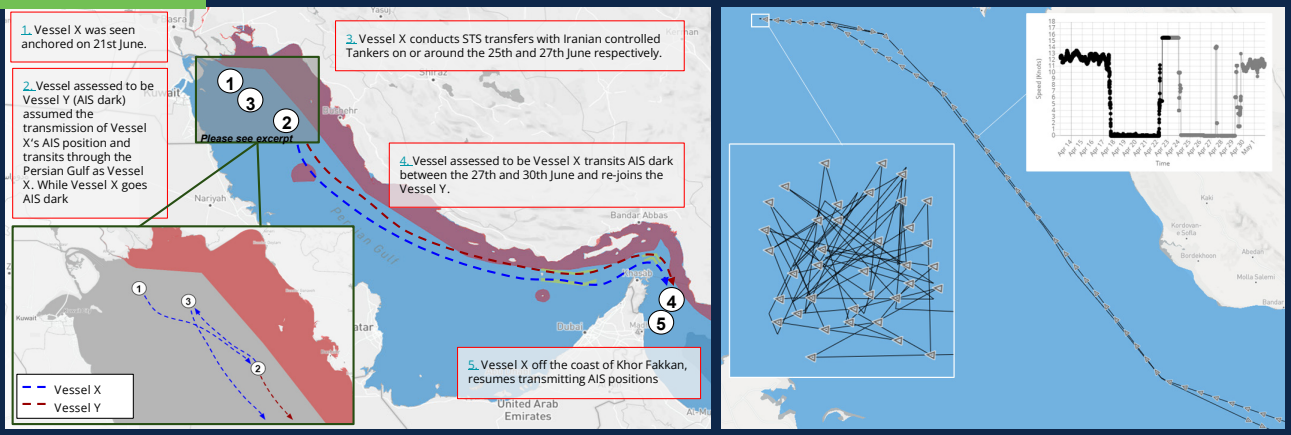


GNSS Manipulation

Transit Examples



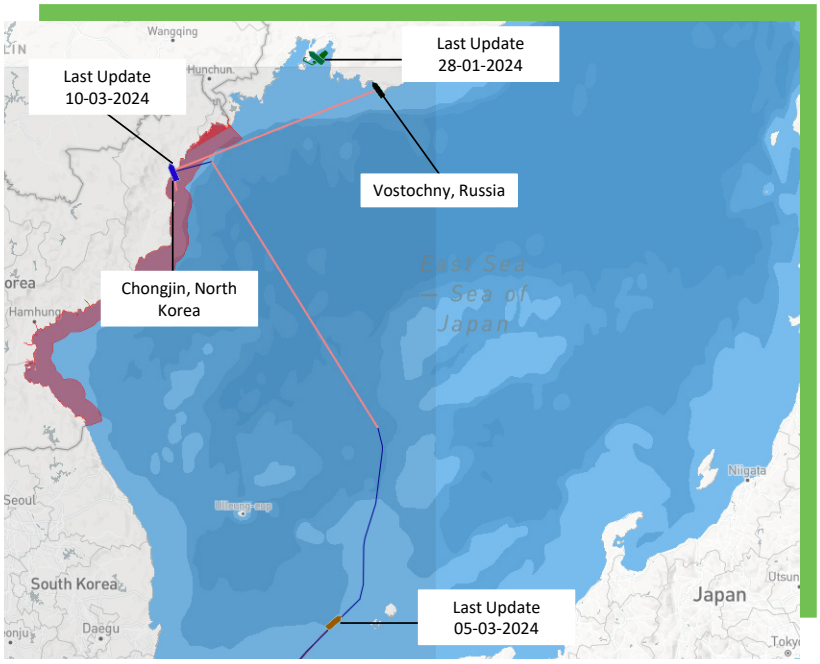
Complex Examples



Manipulation trends

North Korea - Russia

Amidst the ongoing conflict in Ukraine, which has surpassed 24 months in duration, Russia has been actively seeking munitions externally. Reports indicate shipments of munitions from North Korea to Russia, with exchanges involving cargo from tankers, in defiance of UN sanctions have been occurring.



These transactions occur at berths and facilities adjacent to a large container terminal managed by Eastern Stevedoring Company (ООО 'Восточная стивидорная компания'), a part of Russia's major logistics conglomerate, Delo. Both Eastern Stevedoring Company and Transcontainer, also under the Delo group, were sanctioned by the US on February 23, 2024, for facilitating the shipment of munitions from the DPRK to Russia.

With assistance from both Russia and China, North Korean trade in weapons and other sanctioned commodities is increasing, providing Pyongyang with significant revenue and strategic resources it previously lacked. While imports of refined petroleum remain a priority for Pyongyang, recent activities suggest Kim Jong Un's interest in acquiring advanced Russian military technology, as indicated by his recent trip to Vladivostok.

Examining Geonius, vessels in these areas often operate with their AIS turned off, reporting sporadically for extended periods. The following image displays four of these vessels associated with some of these transfers and their last update times. However, instances of advanced anchor circles have been previously identified.

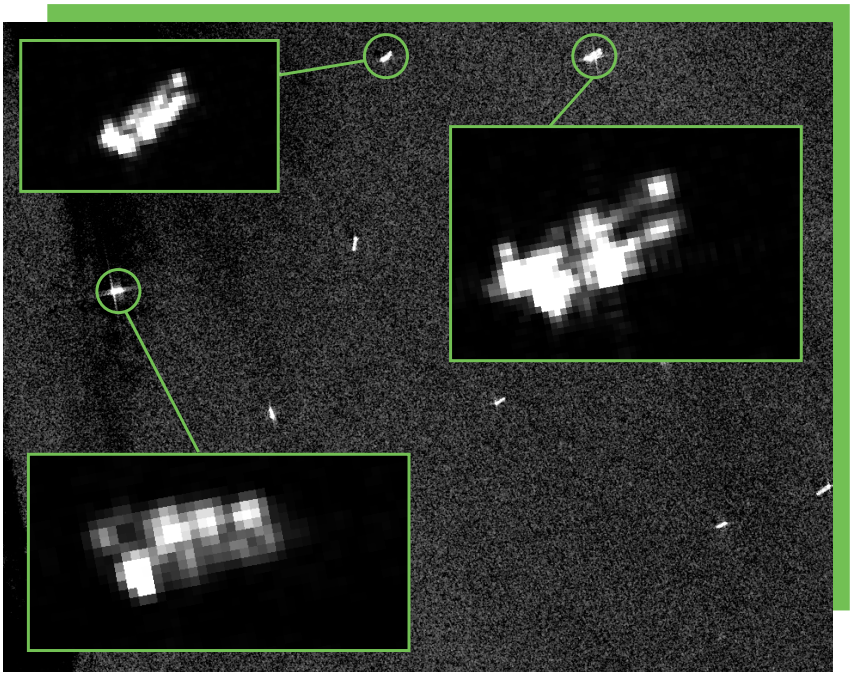
More instances of AIS manipulation within the Sea of Japan have been identified from 2023 to 2024. Vessels previously identified operating in Venezuela have experienced a shift in their areas of movement and are now observed operating in the movement of Russian cargo in this area.

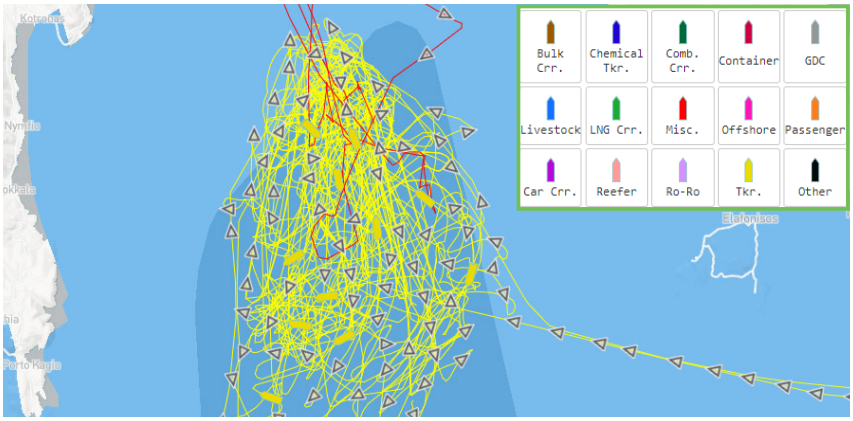
Laconian Gulf - Russia

Ship-to-ship transfers involving Russian cargo are sometimes conducted legally but are also used as a tactic to evade sanctions. The Laconian Gulf is a hotspot for such transfers, with the second vessel often transiting through the Red Sea.

The following Geollect screenshot depicts vessels within the area over a 24-hour period, visualised by vessel type. It reveals that, apart from tankers, only one vessel, shown in red and most likely a tug, was present in the area.

Through the use of Synthetic Aperture Radar (SAR) images taken during the same time period, further vessels not displaying on AIS during this period have been identified. Additionally, at least three instances of ship-to-ship transfers have been observed in the same capture.





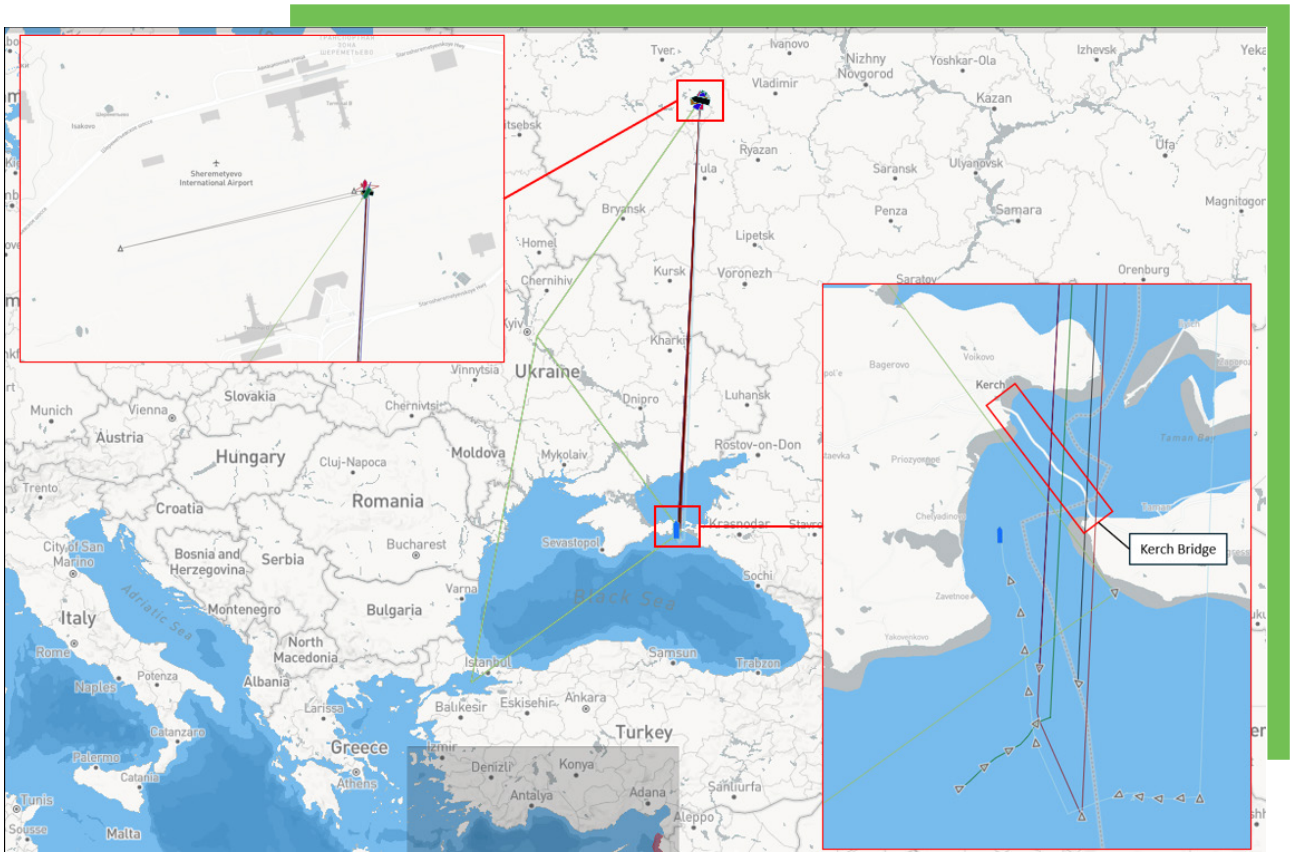
Black Sea - Kerch Bridge

Russia's Sheremetyevo International Airport regularly registered over 60 ships appearing present over the main runway. From tugs to tankers, there has been a significant number of ships transmitting Automatic Identification System (AIS) positions over the airport since November 2023.

Upon closer examination of this series of manipulated positions, Roke uncovered what appears to be a Russian defensive measure aimed at protecting the Kerch Strait Bridge.

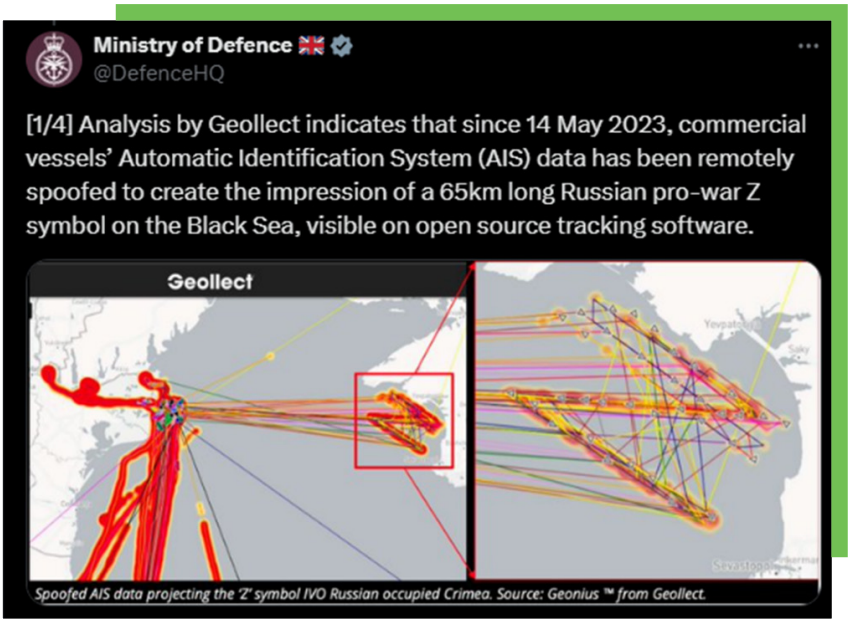
Through the use of mass AIS manipulation, Russia is likely disrupting common navigational frequencies used by Ukrainian naval drones to avoid the bridge being struck during an attack. Due to Ukraine's repeated and successful attempts to target the critical bridge via UUSVs, this would be a logical and novel way of countering this new threat.

Further incidents involving greater number of vessels have been identified in Crimea on the 2nd April 2024, highlighting that these events are becoming more frequent in disrupting navigation in the area.



Black Sea - Sevastopol

In this example, it appears that the spoofing was done deliberately by a pro-Russian actor as either or both an information operation and a demonstration of capability.



The context of this was that the long awaited Ukrainian Spring Offensive was about to begin imminently, and that Russia had failed to prevent Ukraine from importing and exporting via the Black Sea.

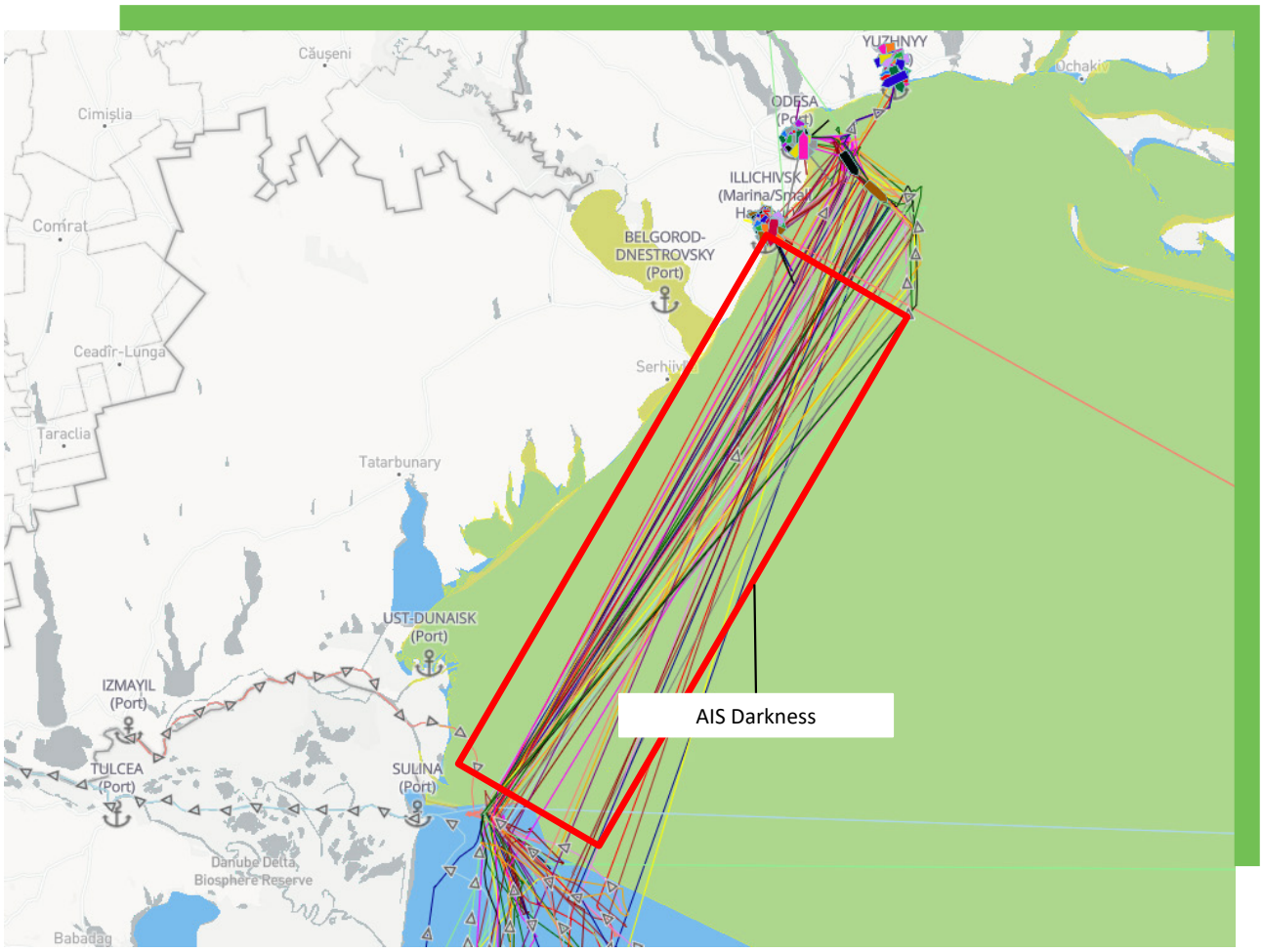
This mass spoofing incident, although historically more prevalent, still impacts vessels in the area, albeit to a lesser extent, particularly in the vicinity of the Sevastopol area. It is likely that this earlier incident of mass spoofing served as a precursor to the current occurrences surrounding the Kerch Bridge.

Black Sea - Odesa

The number of vessels visiting Ukrainian ports has increased in 2024, despite the termination of the Black Sea grain deal. These vessels are observed going AIS dark just outside the Ukrainian Exclusive Economic Zone and reappearing in the vicinity of the Ukrainian ports of Odessa, Chornomorka, and Yuzhnyy.

This is almost certainly to avoid being targeted by Russian forces, however, this practices obscures if a vessel has entered the area or anchoring off Sulina until it resumes transmissions.

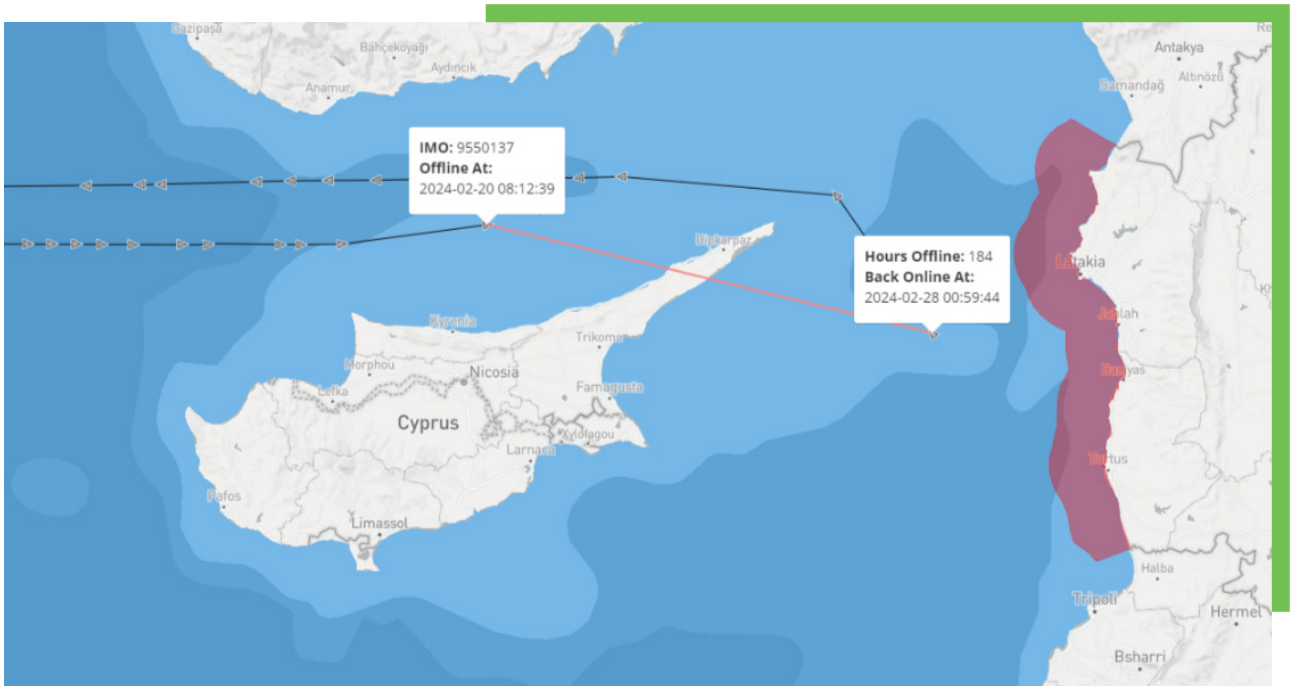
This is also seen in reference to Russian ports, however, this is also obscured by the mass spoofing incident mentioned previously causing interference to vessels.



Syria

In 2024, vessels continue to go AIS dark in the vicinity of Cyprus while entering Syria. They often remain AIS dark for several days before reappearing and heading in the opposite direction. Little AIS manipulation, other than vessels going AIS dark, is observed in the area.

However, recently there has been mass spoofing from this area to an airport in Lebanon. If this trend continues, it may obscure vessel positions in the future.

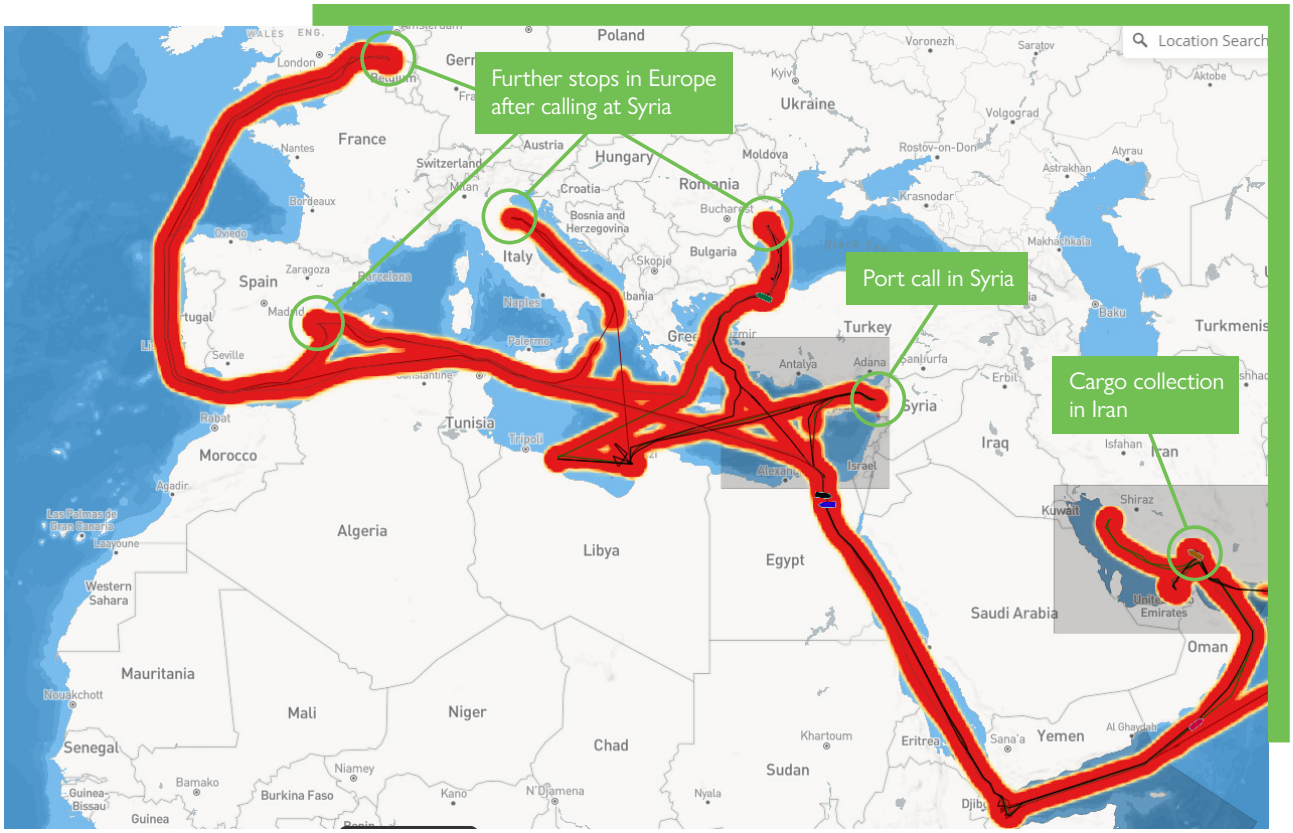


Syria - Iran

Iranian container ships, accused of transporting arms have openly made port calls in Syria before continuing to European ports, allegedly switching cargoes. The practice of this changing containers on route to Europe, particularly under the guise of companies based in countries such as Romania, enables Iran to remain further under the radar and obscure the true purpose of the journey.

It is believed that these shipments to Syria are subsequently transferred to Hezbollah, rather than being transported via land routes, due to the Israeli Air Force targeting of consignments entering via Iraq.

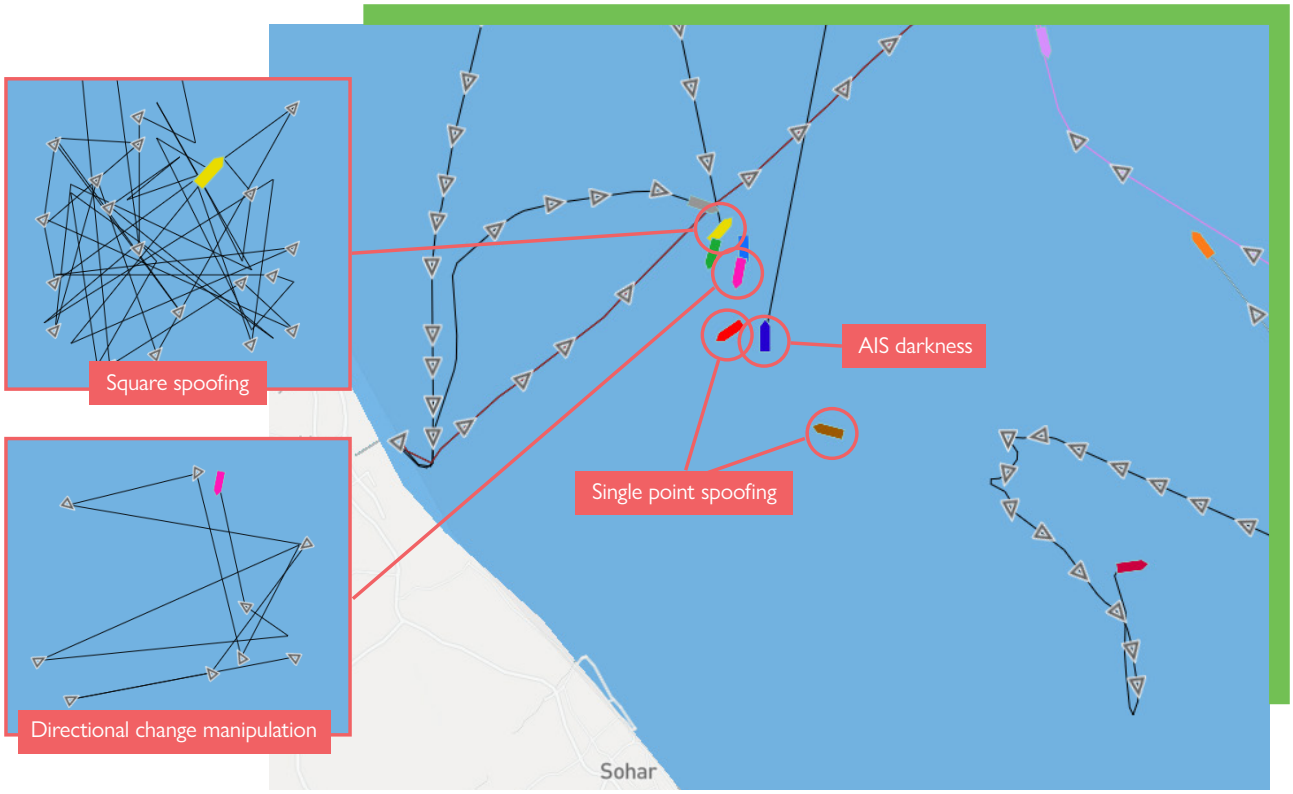
Despite the absence of obvious manipulation in AIS during these transits, it is likely that these vessels are being utilised as a method of concealing arms within cargo shipments originating from Iran and destined for Europe is being highlighted as a deceptive shipping practice currently being employed.



Gulf of Oman - Sohar

A hotspot for AIS manipulation has been identified off the coast of Sohar and Liwa port. These incidents encompass various categories, displaying different levels of sophistication. However, they all involve either basic manipulation or anchor manipulation.

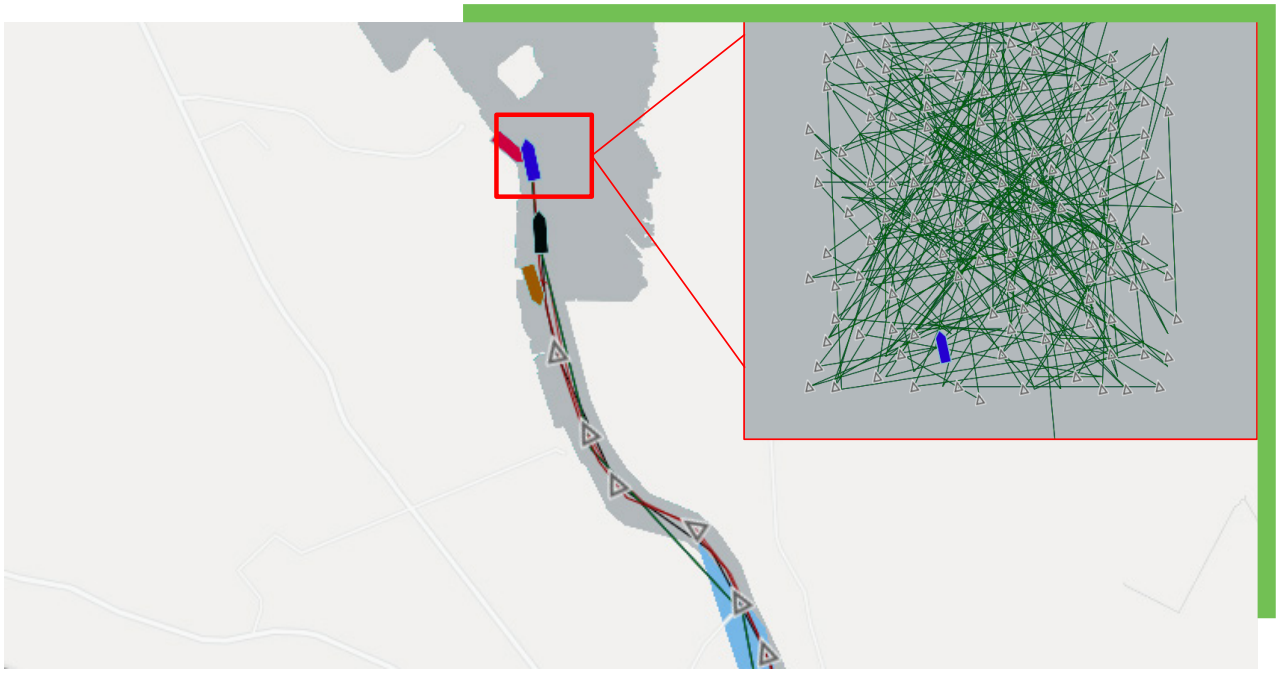
Notably, within this area, an equal number of tankers and cargo vessels have shown indications of AIS manipulation. Furthermore, vessels investigated for manipulation in this area were highly likely visiting Iranian ports during this time.



Persian Gulf - Iraq Ports

An increased amount of manipulation has recently been identified occurring more often with vessels alongside or near port area, the following image shows an instance of this in the last 48 hours in vicinity of Khor al-Zubair.

It is likely that these incidents have been happening more frequently, as vessels heading towards berths or in berthing operations exhibit sporadic AIS positions. These instances can be challenging to identify, as some seem similar to AIS manipulation.

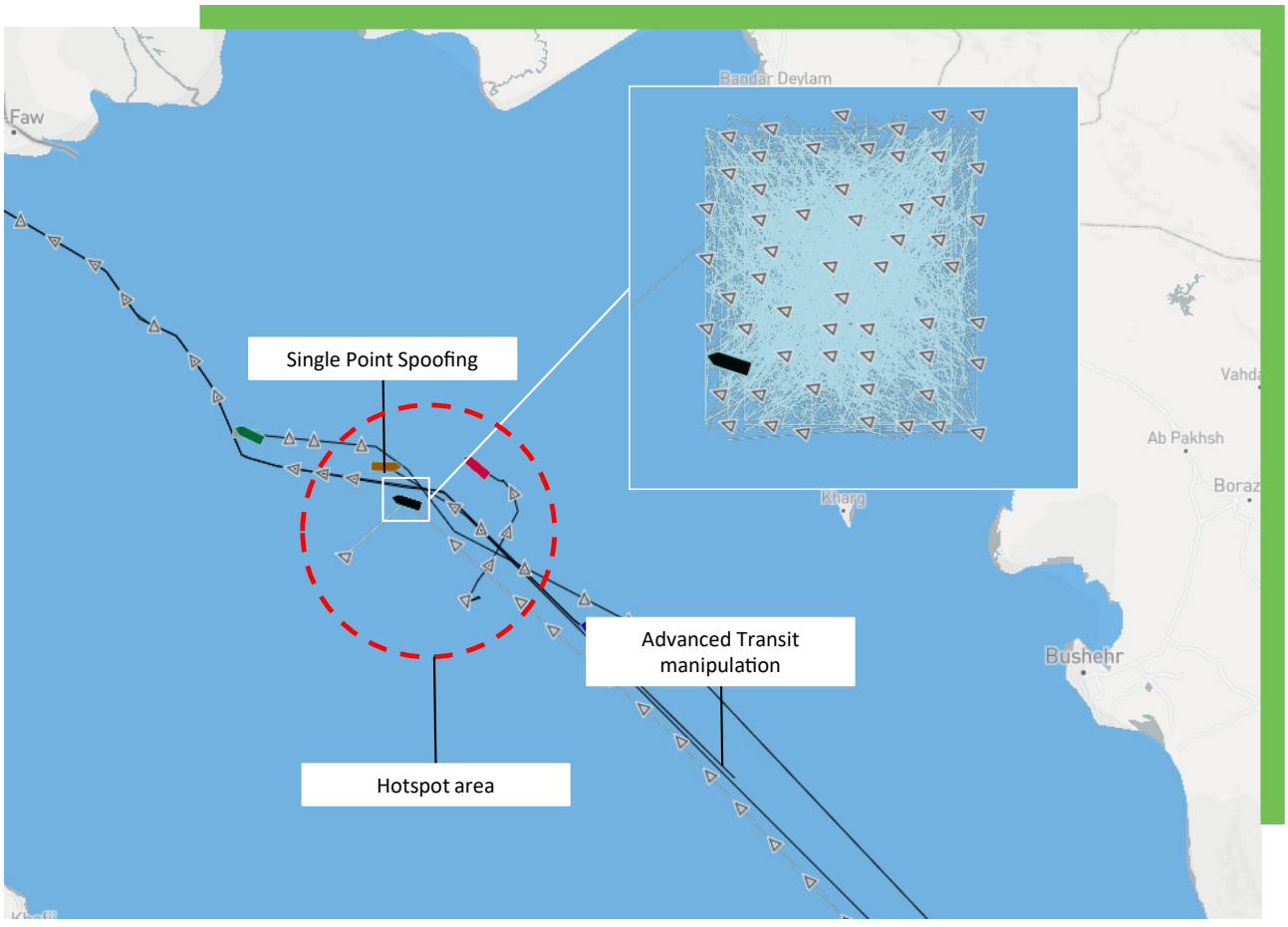


Persian Gulf

The waters of the Persian Gulf outside of country TTW's continue to be a hotspot for AIS manipulation. These manipulations typically take the form of square spoofing, single-point spoofing, and transit manipulation.

However, it is increasingly common to observe a combination of these methods being used in a hybrid manner to obscure the vessel's location for longer periods. There have been very few incidents of advanced anchor manipulation identified in this area, unlike occurrences in the Gulf of Oman and the South China Sea, where such incidents are more frequent.

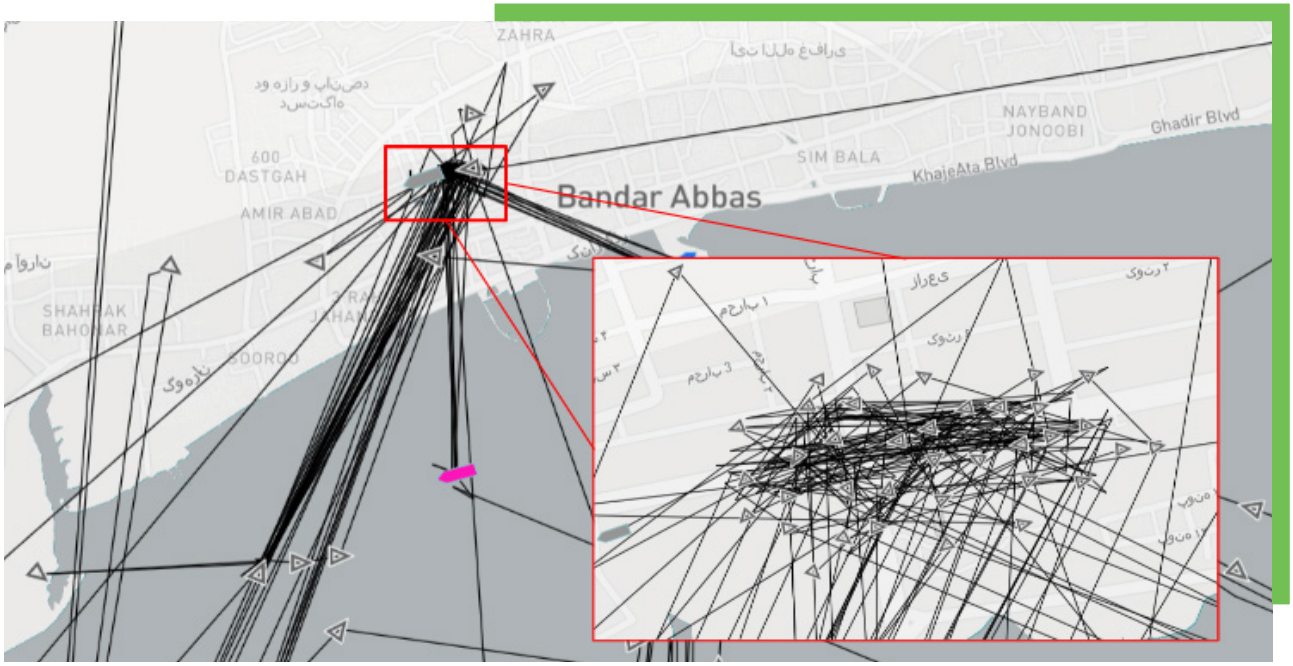
A number of the hybrid incidents start and end with the commencement of Square manipulations In vicinity of Dubai and areas around the offshore terminals of Sirus and Al-Basra Oil terminal likely to obscure cargo origins.



Iran Mass Spoofing

This mass spoofing incident appears anomalous to the other examples, as there was no immediately obvious significance of the focal point to the spoofing.

This could suggest the position was chosen in error, or at random to demonstrate a concept, or that it was being used to have an affect over Bandar Abbas' port.



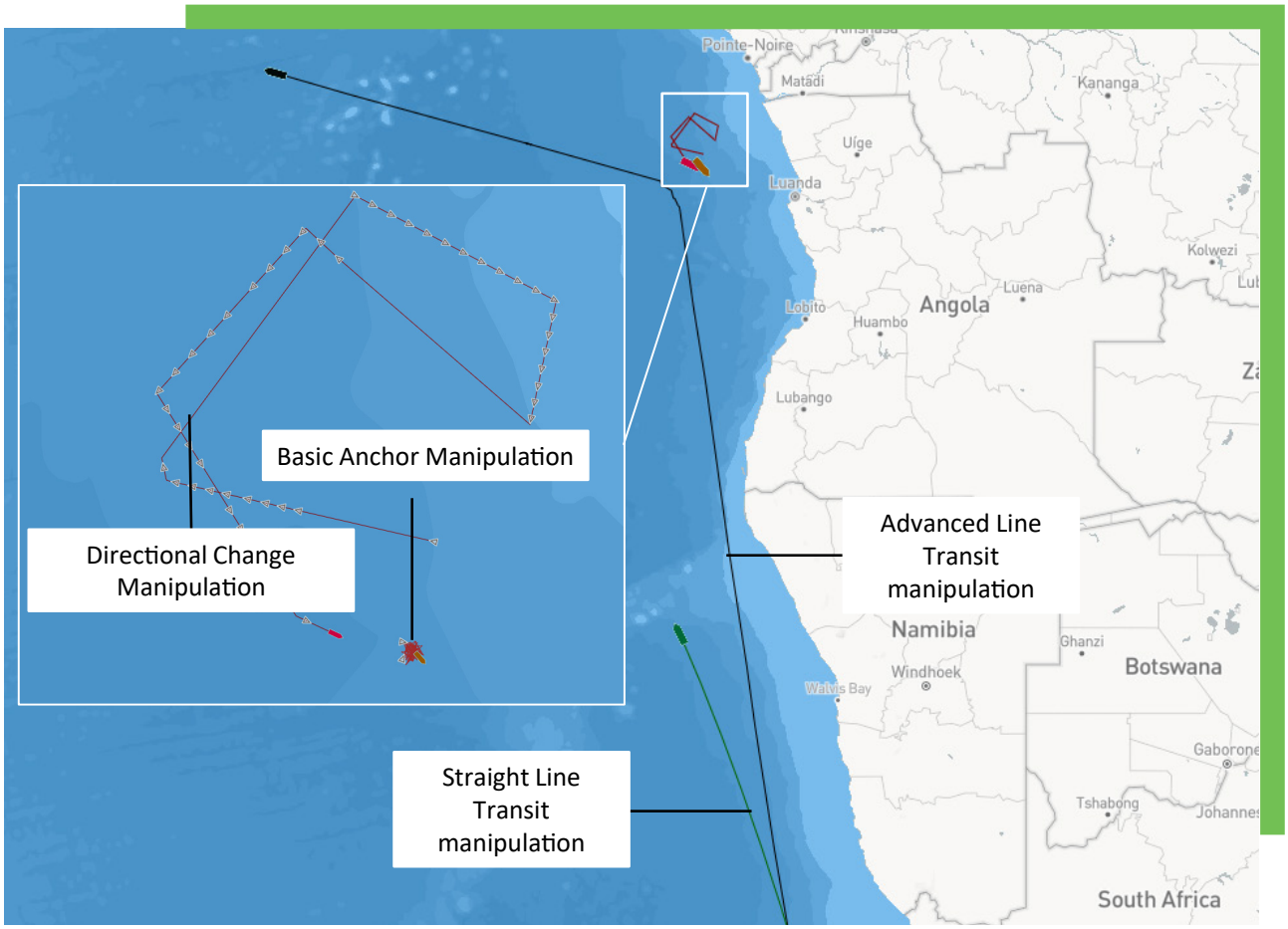
West Africa - Venezuela

Following the relaxation of sanctions on Venezuela by the US, a noticeable shift has occurred in the behaviour of certain vessels previously suspected of manipulating their AIS data within the Caribbean and Atlantic Ocean. These vessels are now openly visiting Venezuelan ports.

Despite this change, there remain several vessels still engaged in manipulating AIS positions in areas west of Luanda and west of Sierra Leone. These vessels are likely visiting Venezuela while operating in AIS dark mode.

The recent developments can be attributed to several factors, including the US's threat to reimpose sanctions on the Venezuelan oil sector in January 2024 and the expiration of the sanctions waiver on the 18th of April.

Manipulations in AIS positions primarily involve transit AIS manipulation, although some instances of anchor manipulations have been detected in closer proximity to Venezuela. These activities raise concerns about compliance with international regulations and potential sanctions evasion.



South China Sea

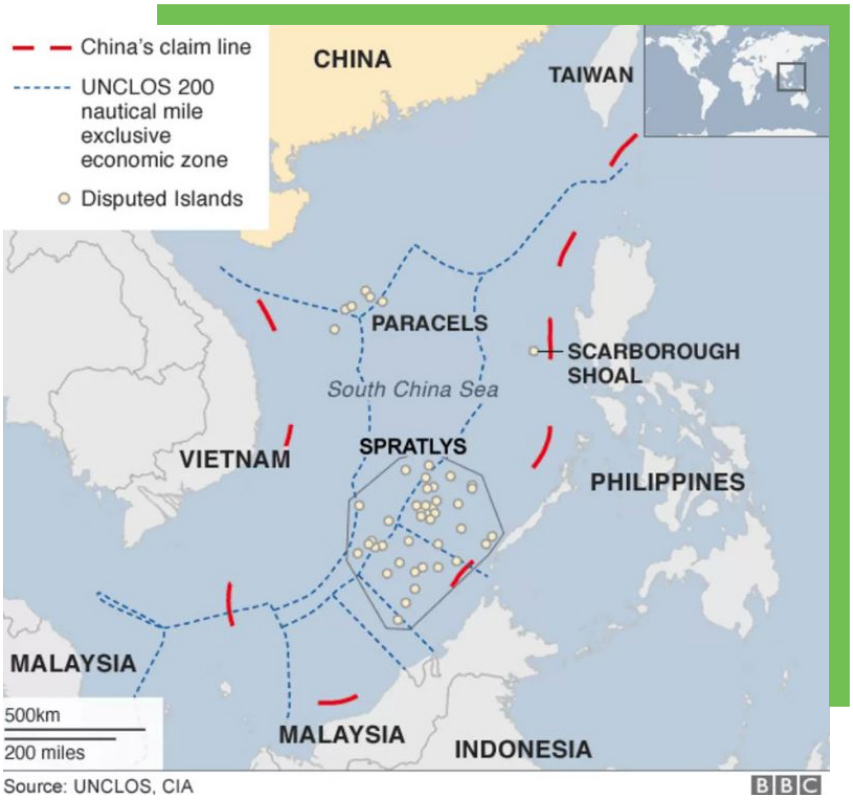
Manipulations in the South China Sea off the coasts of Malaysia and Singapore tend to be more advanced. These involve either utilising sophisticated manipulated transits or engaging in ship-to-ship transfers in areas with large gatherings of vessels, where one vessel remains dark while the other displays legitimate AIS signals.

Despite this, there have been instances of less advanced manipulations, albeit to a lesser extent. The screenshot displayed shows one such incident, depicting a vessel seemingly jumping a distance that is physically impossible to transit, along with exhibiting a square spoofing pattern at Port Dickson.

Chinese Coast Guard South China Sea

Throughout the summer and fall of 2023, People's Liberation Army Navy (PLAN) and China Coast Guard (CCG) vessels have repeatedly blockaded Filipino shoals and naval outposts in the South China Sea, restricting freedom of movement and preventing resupply efforts.

These vessels have been seen not transmitting AIS and in some instances corroborated with open source information have been identified in manipulating there AIS to disguise their identity as other vessels.



ROKE

We believe in improving the world through innovation. We do it by bringing the physical and digital together in ways that revolutionise industries.

That's why we've fostered an environment where some of the world's finest minds have the freedom, support and trust to succeed.

Roke is a team of curious and deeply technical engineers dedicated to safely unlocking the economic and societal potential of connected real-world assets. Our 60 year heritage and deep knowledge in sensors, communications, cyber and AI means our people are uniquely placed to combine and apply these technologies in ways that keep people safe whilst unlocking value. For our clients, we're a trusted partner that welcomes any problem confident that our consulting, research, innovation and product development will help them revolutionise and improve their world.

If you're bringing the physical and digital worlds together, we'd love to talk.

Roke Manor Research Ltd
Romsey, Hampshire, SO51 0ZN, UK
T: +44 (0)1794 833000
info@roke.co.uk www.roke.co.uk