WINDWARD

The location illusion: How to manage risk in the age of GNSS manipulation

Table of Contents

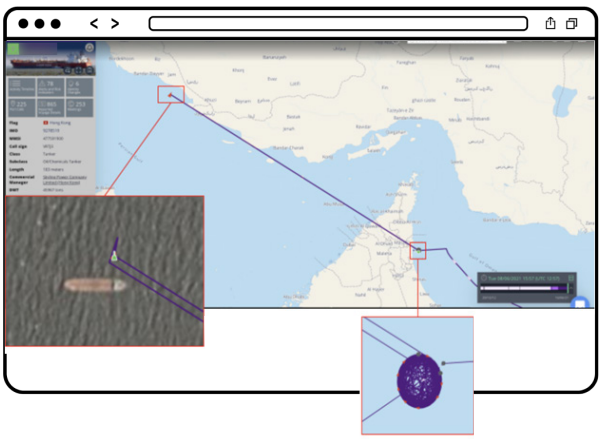
INTRODUCTION

Last year, the OFAC and the OFSI advisories provided guidance for the industry on maritime red flags - specifically coined by the UN Panel of Experts, as deceptive shipping practices. Deceptive shipping practices are tactics commonly used by bad actors to avoid sanctions or disguise illicit trade. Suddenly terms like “dark activity” (i.e. intentional disabling of AIS transmissions) and ship-to-ship transfers became common terms for compliance analysts worldwide as the market reacted by introducing new clauses and due diligence processes. And bad actors were just as quick to react.

As early as August 2020, just three months after the published advisories, Windward saw instances of GNSS manipulation methods to overcome the industry’s development. These methods are done within the same realm of AIS that has accompanied the shipping industry since the 80’s. And while AIS hasn’t seen major advancements, bad actors have attained technologies and know-how that have enabled them to co-opt electronic warfare manipulations that up until now were only in the hands of states.

By using machine-generated location tampering, bad actors falsify the GPS reading transmitted via the AIS device to transmit a different location than the vessel’s real whereabouts. Deceptive shipping practices, like GNSS manipulation, can create an illusion of knowledge and without strong technology and the right insights, stakeholders can be left in the dark. What does this look like in practice? Take the case of Vessel A** - the vessel appears to be ‘drifting’ offshore the UAE. Upon a closer look however, the synthetic patterns indicate a machine-generated drifting pattern. Further, the vessel was not even in the UAE. It had a positional jump (a possible technical malfunction by the bad actors), positioning it in fact, within Iranian waters.

**Vessel name was changed for anonymity



This is a prime example of how such cases confound true events at sea. The truth is that GNSS manipulation has reached a point where it is nearly impossible to detect. Any vessel crossing the Suez canal or drifting offshore the UAE might actually be in Syria, Iran, or anywhere else in the world. Even more troubling is that these aren’t isolated cases.

In this whitepaper, we’ll discuss how GNSS manipulation has taken the maritime domain by storm, evolving faster and posing a greater risk than any other deceptive shipping practice seen before. The scale of the problem is one that compliance professionals simply cannot leave unmanaged.

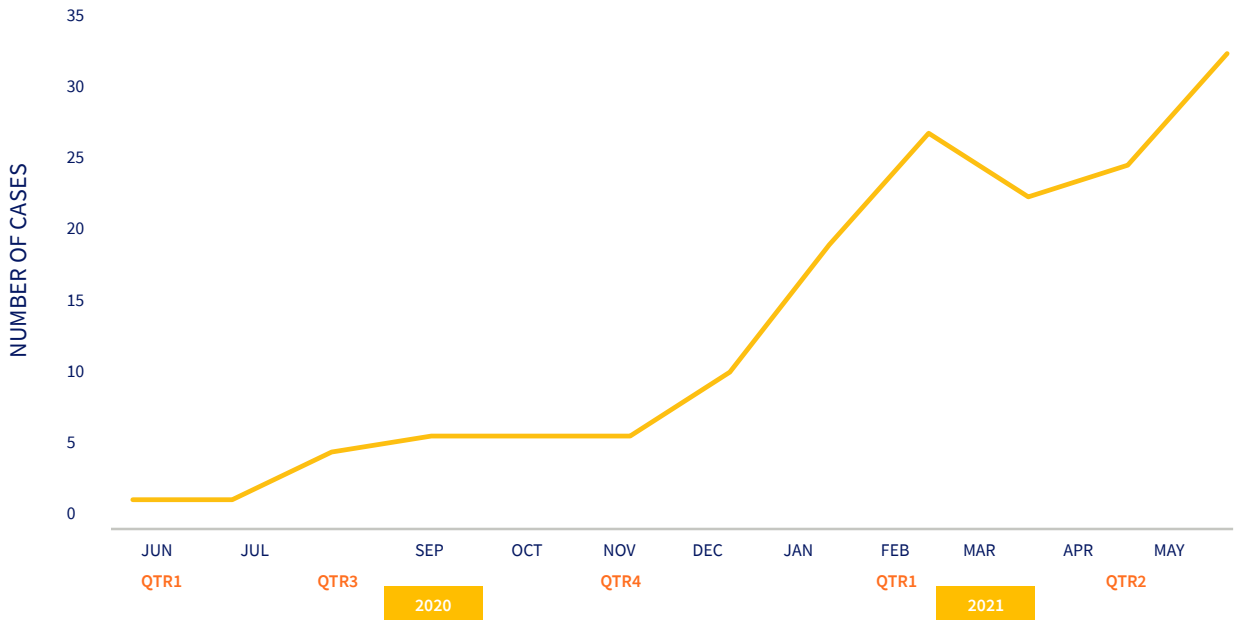
A DIFFERENT PLAYING FIELD

Over the years, with the development of MDA systems and enhanced surveillance tools, dark activity has become commonplace. This practice, done to disguise the true location and activity of a vessel, is effective, but not sophisticated. Today, it is still executed as it was 5 or even 10 years ago. In contrast, GNSS manipulation has not only seen exponential growth, but it looks completely different with every month that passes. Each case is more advanced than the last. What began as distinguishable machine-generated patterns, has begun to look more and more like natural sailing paths.

At Windward, we're long familiar with bad actors' habit of imitating vessel behavior in order to appear legitimate and bypass detection. At first, dark activity was the name of the game. But since dark activity has been around for so long, when a vessel turns off its transmission, any tracking system is quick to red-flag it. On the other hand, GNSS manipulation is much more likely to go undetected. The impact? According to our research, just from Q2 of 2020 to Q2 of 2021, there has been a **5000**% increase in GNSS manipulation cases.

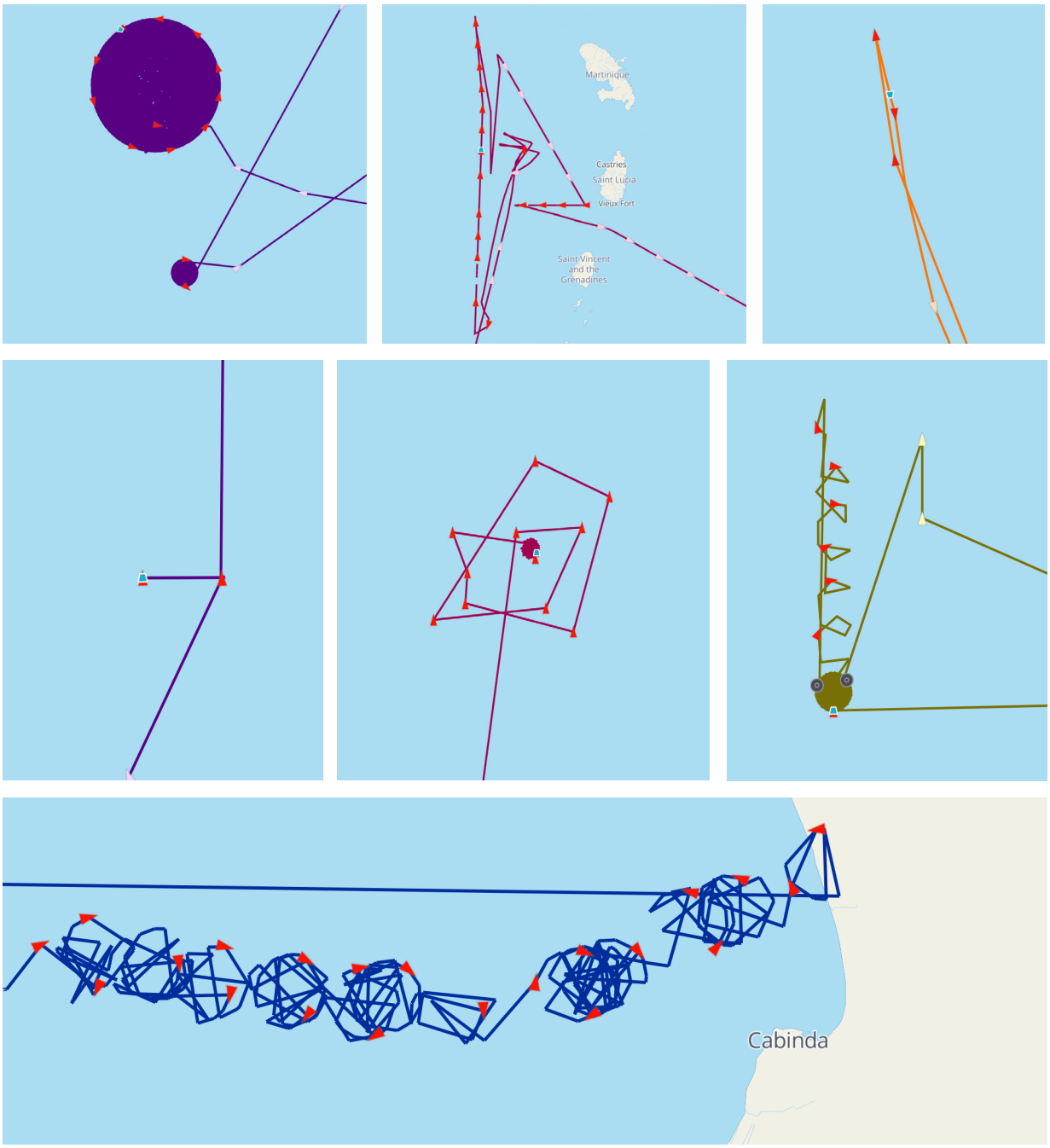
The May 2020 advisory demanded a higher level of due diligence, and the market reacted by onboarding advanced systems. Nevertheless, the counteraction by bad actors was faster, and more sophisticated, than expected. With advanced manipulation tactics on the rise, a business as usual approach will fall short in effectively managing risk in this environment.

THE SCALE OF THE PROBLEM



When the OFAC advisory was published in May 2020, GNSS manipulation was not on any compliance or security radar. But very quickly, cases started to emerge. At the time, many players in the market were unable to explain the developing phenomenon. Since we have recorded cases from over a year ago, we wanted to compare how GNSS manipulation fared since the OFAC advisory in May 2020, to understand if enhanced regulations perhaps triggered a rise in cases. In May 2020, there were no detected cases of GNSS manipulation. Windward data then shows a sharp increase in cases beginning in June and continuing throughout the year. From May 2020 to May 2021, the number of unique vessels and cases **almost doubled** the amount. In this time period, there were 98 unique vessels that had manipulated their location or ID. There were over 140 unique events with instances of vessels employing this practice. In the graph above, you can see the rapid rise in cases identified by our models.

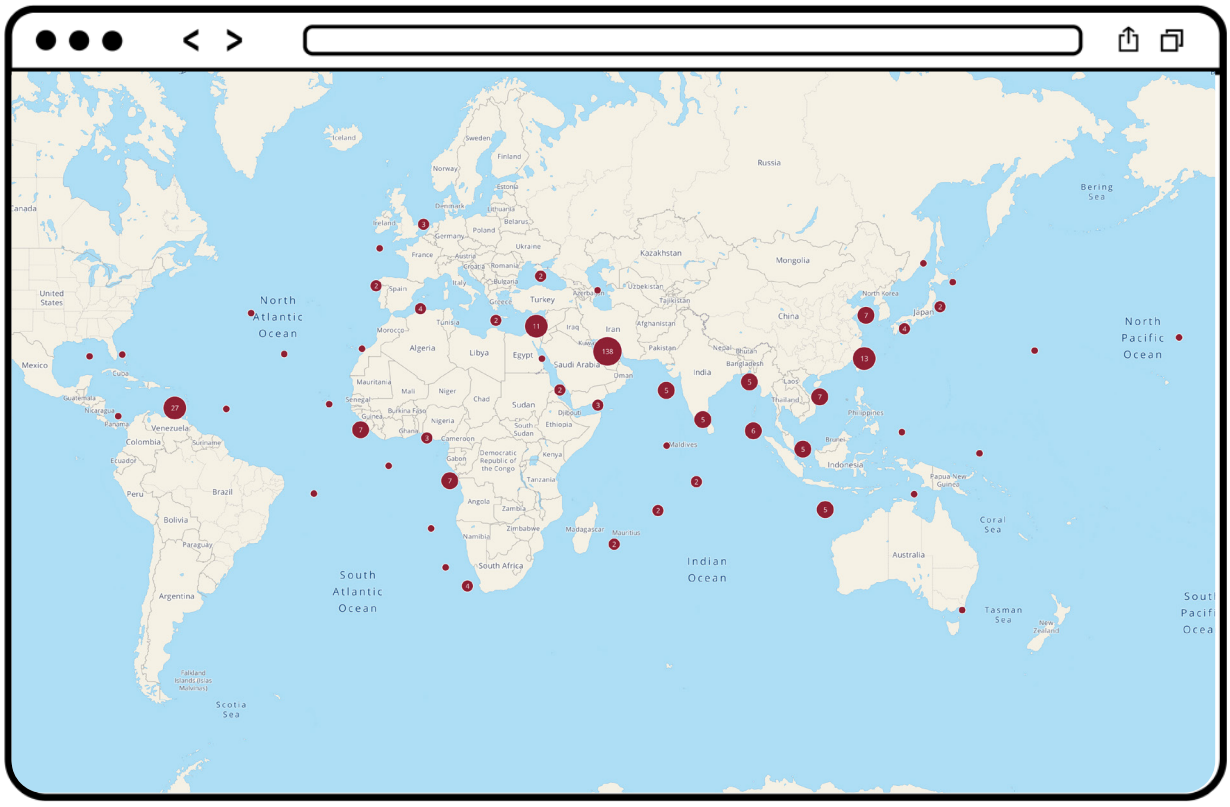
But it doesn't end there. Since May 2021 and until the end of August 2021, we've seen an additional 80 unique vessels and 95 unique events of GNSS manipulation. This is nearly the same number of cases seen over the course of one year - **in less than half the time.** So rather than a fleeting trend, it's clear that this tactic is becoming an alarming norm.



Without the ability to detect cases like these, stakeholders are left blind. If the vessel isn't where it's claiming to be then where is it? What activity is going undetected? What is the motivation behind it? Are there other vessels involved in the operation? Are the port authorities aware? Is the flag registry? Or what about the owner and insurers of the vessel? Leaving these questions unanswered can leave risk unaccounted for.

REGIONAL TRENDS

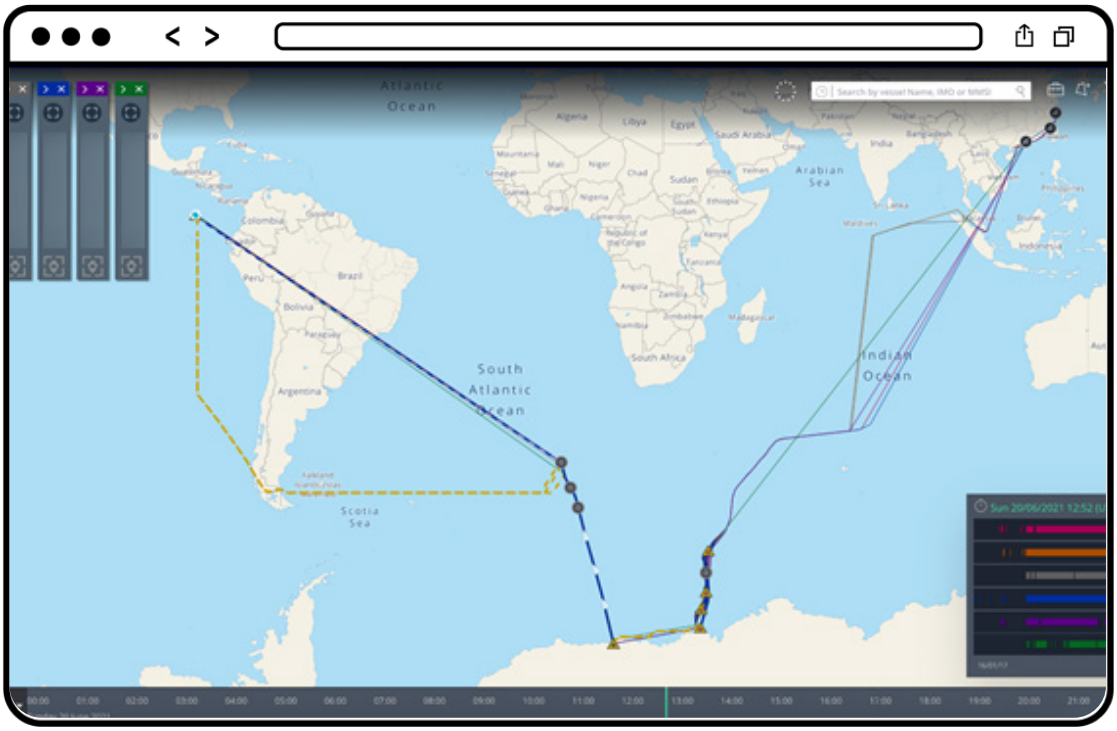
When looking at regional trends - the correlation of identified cases of GNSS manipulation to sanctioned regimes can be easily seen. In the image below, you can see that the major clustering of these manipulations are related to sanctioned regimes. This makes sense, as sanction evaders seek to disguise the shipment of sanctioned commodities and maximize the success of their smuggling networks. Most notably - the largest cluster of cases can be seen in the regions of the Caribbean and the Persian Gulf.



But it's important to mention that the technology employed today by bad actors is not limited to sanctions. In fact, Windward has detected events of GNSS manipulation that go beyond the realm of compliance. Bad actors don't distinguish the use case – their goal is to go undetected, and GNSS manipulation is highly effective to this end.

The Fishing Fleet

With sanctions evasion, at least the intention behind GNSS manipulation is clear. But what about other vessel types? What would it mean for a cargo vessel or fishing vessel to employ this method of disguise? Windward recently detected six Chinese fishing vessels manipulating their location. The fleet has operated together and conducted the same voyages over the past year - with their current “location” on the South Atlantic Ocean as seen in the images below. These are Chinese vessels transmitting a location West of Panama while not physically being there - allowing them to roam international waters, undetected.



Without the ability to identify these cases at scale, bad actors will continue to reap the rewards of their efforts. And the possibilities for exploitation are endless. The full extent of what GNSS manipulation can be used for - is still unknown, but the first step is knowing exactly when it is happening, where, and what vessels are involved. In this way, compliance and equally, intelligence teams, can evaluate each event, in the right context, and act accordingly.

WHAT THIS MEANS FOR YOUR BUSINESS

One important question to consider is, if you have a system that can detect other deceptive shipping practices like flag hopping or dark activity, isn't that enough? Not exactly. In some cases, GNSS manipulation is the only risk indicator of a vessel. Take the case of a vessel, whose name we will keep anonymous, has no other risk indicators other than location and ID tampering. Prior to January 2nd, 2021, the vessel had no indications of deceptive shipping practices. It operated mainly in the US, then deviated from its pattern and sailed to the Persian Gulf for the first time in December. Shortly after, it manipulated its location. Without this information, why wouldn't you charter this vessel if there were no indications of dark activity? In this context, false positives can expose your business to high-risk deals or transactions.

This vessel is high-risk in our system, but in many cases bad actors take advantage of the fact that many systems in place today are not yet attuned to detecting GNSS manipulation. In fact, they often choose specific vessels due to their innocent appearance and clear background.

A system that can go beyond standard deceptive shipping practices and identify the latest risk trends is critical to meet the sophisticated standards of maritime risk management today. As bad actors continue to take advantage of advanced technologies to cover their tracks, this will be as important as ever.

The May 2020 advisory sent the industry looking for solutions for behavioral indicators, which meant that bad actors had to quickly find ways around this. And they were able to do just that. Maritime risk is fluid. If it's stopped in one place, it'll move to another. It's a long-term game. By leveraging strong tools that can detect manipulation at scale, stakeholders can be one step ahead. With GNSS manipulation continuing to evolve, this will be key to ensuring safety at sea and protecting against larger security threats, globally. And while we can't say for certain what new technologies will be employed by bad actors, we can say one thing for certain: it doesn't end here. As the industry continues to enforce security and compliance measures, those that it works against, will always find new ways to turn a profit.

CONCLUSION

Vessel operations at sea shouldn't be a guessing game. The exact whereabouts of a vessel are key to understanding the intentions and nature of any maritime incident or event. That's why GNSS manipulation is such a threat to the industry. And it impacts every stakeholder across the industry. Why? The applications are infinite when it comes to what activities or operations can be executed when a vessel's true location is well-disguised. And this past year has proven just how quickly and effectively this can be done.

The time to act is now. Bad actors will continue to try to fool and get past traditional maritime risk solutions. By automatically identifying when they act next, stakeholders can respond in real-time, before the damage is done. Learn more at **windward.ai**