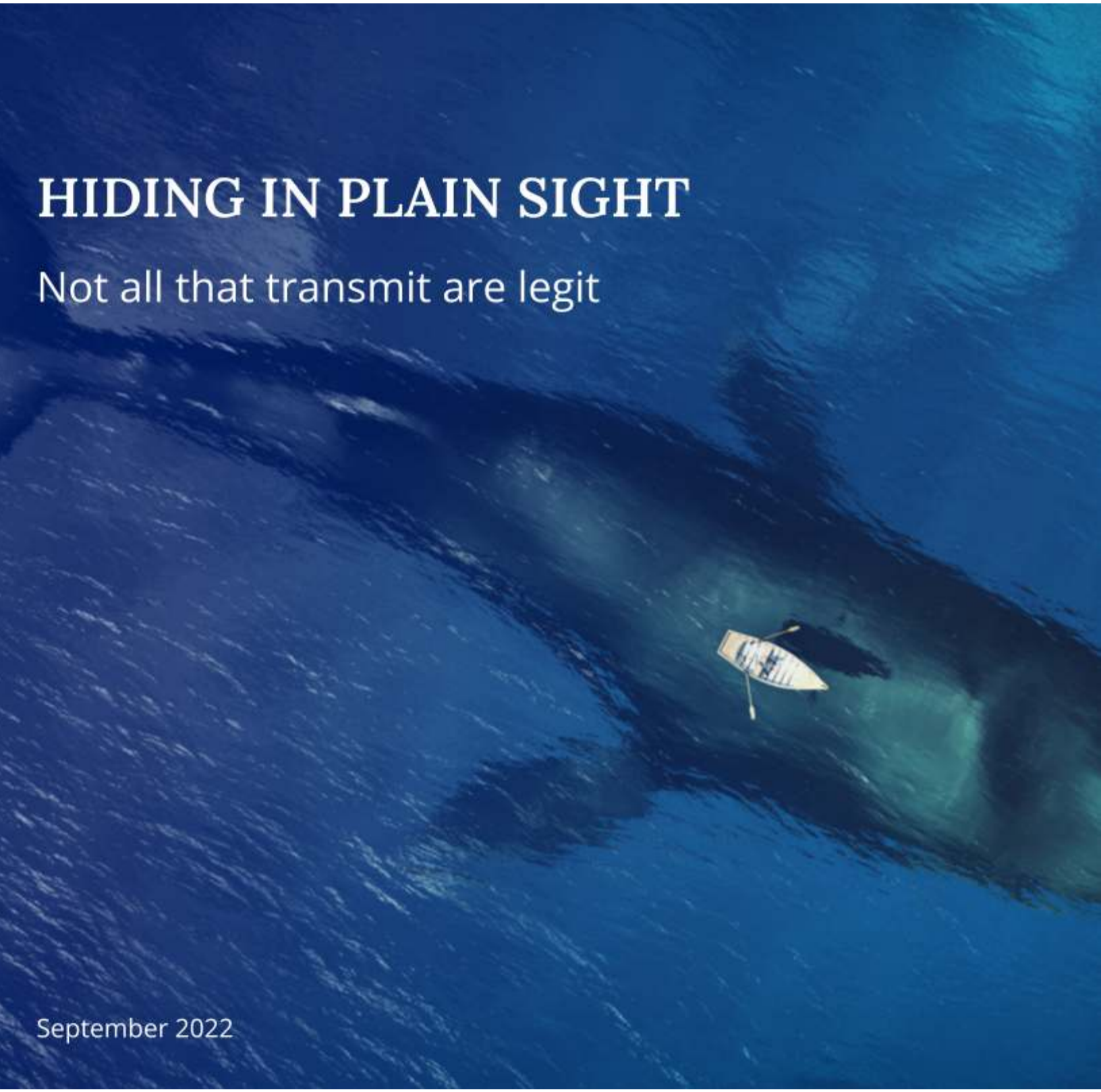

HIDING IN PLAIN SIGHT

Not all that transmit are legit

September 2022

Content

Hiding In Plain Sight

Deceptive shipping practices have existed since the beginning of commercial shipping. Way back in the 17th century, pirates used neutral flags to mask their true identities and fool potential victims. The more things change, the more they stay the same in terms of the desire to deceive. Vessels are still changing flags to disguise their true identities, but that is of course far from all that they are doing…

The rules of the maritime detection game (along with the terminology and technology) have changed. "Going dark" (disabling the AIS system) is still popular, but sophisticated bad actors now understand that a vessel worth millions of dollars is too expensive to risk going dark for a single transaction. If identified, the vessel, crew, and owners will not only be exposed to sanctions, but will also suffer from seized cargo and lasting reputational damage. And having a vessel idle for a long period of time could prove costly.

Instead of trying to conceal vessel behavior, many bad actors have changed direction. They now seek to reap the benefit of illegal activities while projecting a veil of "business as usual." In other words, **they are hiding in plain sight**.

New tactics have emerged, making identity changes look as quaint as a 17th century tactic. An umbrella term called "spoofing" has been driving the maritime industry crazy with multiple interpretations. Within this concept, there are multiple tactics involving the use of various identities, transmitters, and even GNSS manipulation methodologies that are growing at an exponential speed compared to previous deceptive shipping practices.

And the U.S. Treasury Department's Office of Foreign Asset Control's (OFAC) early guidance on implementation of a **maritime services policy for seaborn Russian oil** was a recent reminder that the stakes are high. Entities throughout the maritime ecosystem are expected to be able to track and flag abnormal shipping routes or transshipments, and know who they are doing business with.

This whitepaper aims to make it easier for you to find the hiders by explaining the new deceptive shipping tactics; quantifying the amount of location tampering worldwide, based on Windward's AI-driven insights and research; and presenting real-life use cases of vessels that seemingly would do anything to evade sanctions unnoticed.

From identity tampering to "AIS handshakes" **and a new concept we are introducing, "zombie vessels,"** Windward will expose the tactics currently outwitting the overwhelming majority of marine domain awareness (MDA) systems.

Terminology

Before discussing the evolution of deceptive shipping practices, it is important to quickly define terms to ensure there is a standardized conceptual framework. The industry tends to group many different activities as “spoofing,” which is too general and leads to confusion. To truly and accurately identify and mitigate these risks, we must first define them to understand exactly what we are looking for and how it's done.

We have divided up this chapter of the white paper into three sections:

- **The Classics** – the tried and true techniques that have seemingly been around forever
- **Identity Games** – newer deceptive practices that we are seeing more frequently
- **Seafloor Strategies** – cutting-edge techniques

Creatures that hide on the seafloor have mastered the art of hiding from predators, despite being in plain sight. The “Seafloor Strategies” section describes the latest, most advanced camouflage tactics discovered by Windward’s Maritime AI™ technology and experienced experts. Please feel free to tell us what you think of these concepts and terms via our social media channels.

The Classics

Dark activity – an automatic identification system (AIS) transmission gap intentionally caused by the vessel’s crew to conceal an operation

Identity change – a change in the vessel’s maritime mobile service identity (MMSI), usually accompanied by a change in additional identifiers, such as the name and call sign

Identity Games

Identity tampering – the deliberate falsification of a vessel’s broadcasted data on AIS and/or alterations to its physical features, to misrepresent its identity (from C4ADS (2021). *Unmasked – Vessel Identity Laundering*)

Identity theft – when one vessel assumes the identity of another operating vessel, creating a duplication of the same transmitted identifiers

Identity laundering – when one or more ships deliberately tamper with or misrepresent aspects of their physical, digital, and registered identities. This is done to obfuscate the original identity and necessitates at least one ship assuming a fraudulently obtained, IMO-registered “shell” identity. In a type 1, or “direct” laundering operation, the “dirty” vessel directly assumes the shell identity. In a type 2, or “indirect” operation, a “clean” vessel assumes the shell identity and the dirty vessel assumes the clean vessel’s now-vacant identity (from C4ADS (2021). *Unmasked – Vessel Identity Laundering*)

NOTE: “dirty” in this context refers to a vessel subject to public derogatory reporting, or law enforcement action that may inhibit its ability to engage in commercial operations at will. “Clean” refers to a vessel that has not been the subject of derogatory reporting or law enforcement action that would inhibit its ability to engage in normal commercial activity. So-called “dirty” vessels may masquerade as clean vessels to conduct activities that would be prohibited or difficult under their own identities. (from C4ADS (2021). *Unmasked – Vessel Identity Laundering*)

Dual transmission – the use of multiple AIS transmitters onboard a single vessel transmitting different entities with separate International Maritime Organization (IMO) numbers

Flag hopping – repeatedly changing transmitted MMSIs (flags) to avoid detection. This practice is also used as a legitimate financial tactic, making it difficult to label as an illicit activity

Seafloor Strategies

AIS handshake – the use of a decoy vessel as a disguise. The dirty vessel will assume the clean vessel’s identity as they are sailing at close proximity, while the clean vessel makes its way to its destination while dark. Upon returning, the vessels will recreate the switch, leaving the clean vessel unscathed

Zombie vessel – the use of a scrapped vessel’s identity to perform illicit operations without legal repercussions

Location tampering (global navigation satellite system manipulation) – the use of a machine-generated location/path to disguise the true location of the vessel. Multiple methods have been identified to carry out this deception, including false transmission onboard the vessel and third-party onshore accomplices

Exponential Growth

Since uncovering the location tampering (GNSS manipulation) methodology in early 2021, Windward has seen a fast-growing number of cases. Nearly **600 unique cases** of location tampering have been identified taking place globally, with the majority (56%) occurring near Iran.

Image 1: Global locations of location tampering

As can be seen in the graph below, the exponential growth of this new, sophisticated typology is clear.

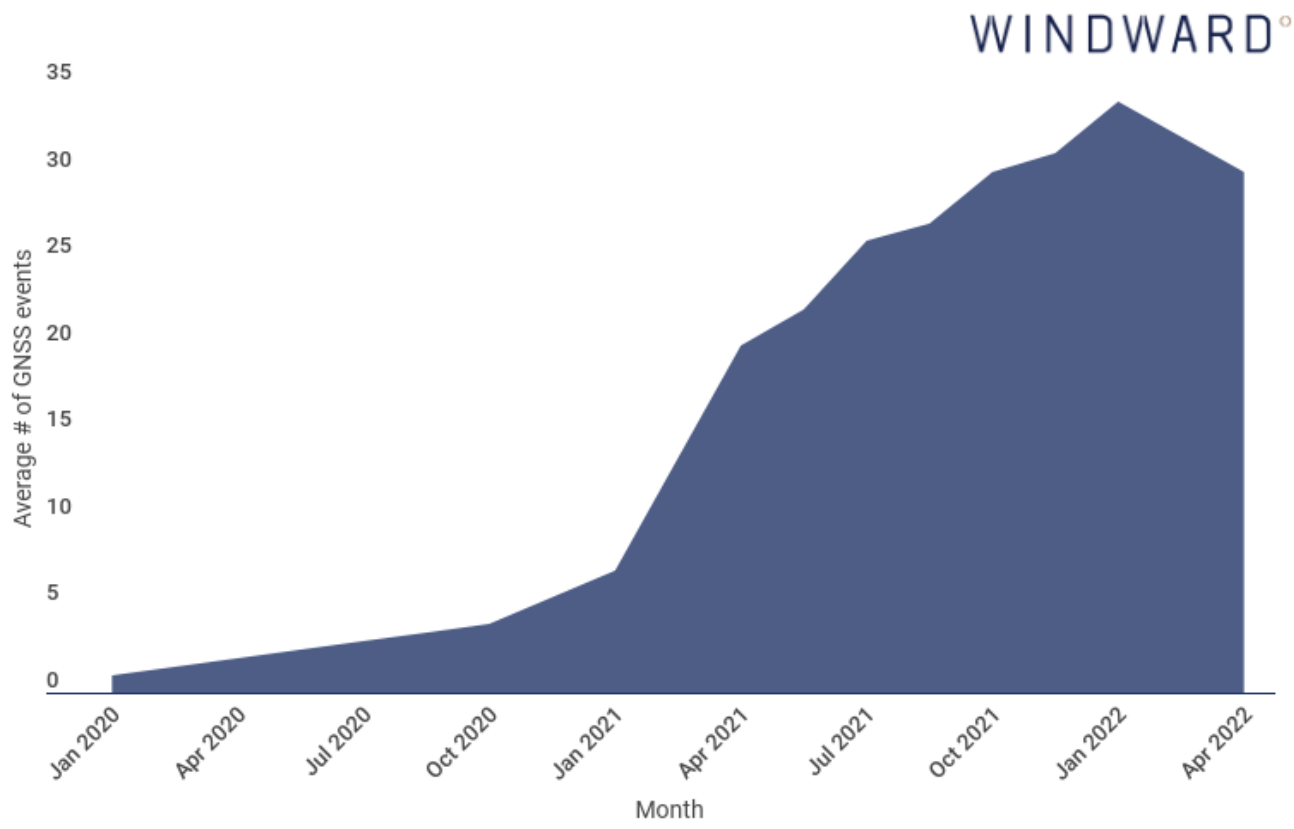

Figure 2: Average number of GNSS manipulation cases per month has spiked since 2020

When we break down the data by vessel class, it becomes clear that this type of illicit behavior is being used for one main purpose – oil smuggling. Out of the 265 unique vessels that conducted the 600 GNSS events, 97% were tankers, followed by 1.5% fishing vessels, and 0.75% cargo vessels.

WINDWARD

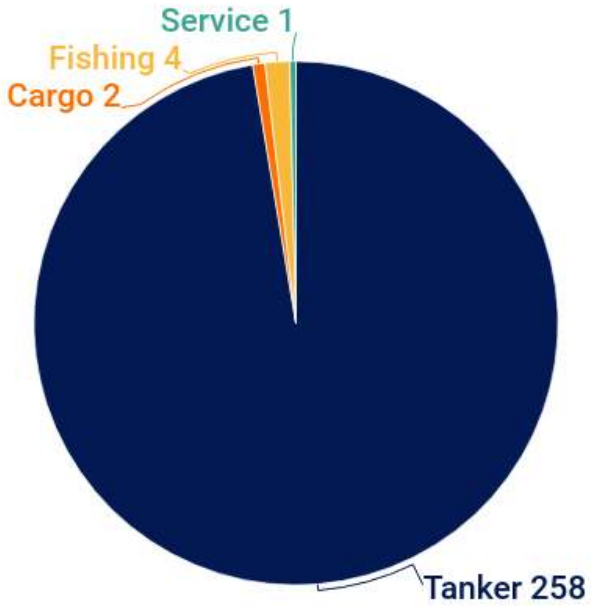

Figure 3: Distribution of the different vessel classes involved in location tampering

The flag distribution shows a pretty clear enabler for this type of behavior. While the distribution spreads across 34 different nations, **77.7%** of them are **flags of convenience**. Windward's data shows that **31%** of the 600 location tampering cases **sailed under the Panama flag** during the manipulation incident(s), **11% under the Liberia flag**, and **8% under the Cameroon flag**.

WINDWARD

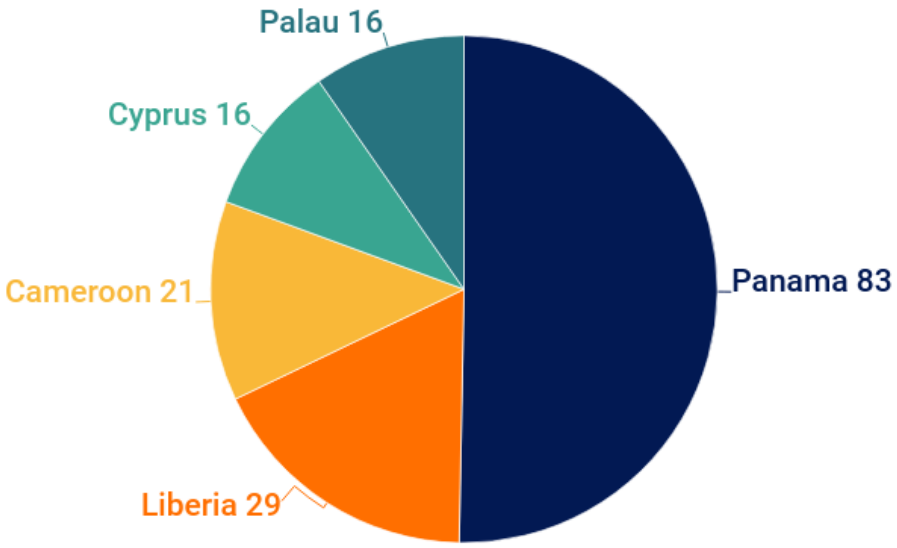

Figure 4: Top 5 flags engaged in GNSS manipulation

In comparison to the GNSS manipulation trend, dark activity has a much steadier monthly growth rate. Since dark activity is easy to execute and is widely used by vessels of all classes and sizes, Windward does not expect it to decline in the near future.

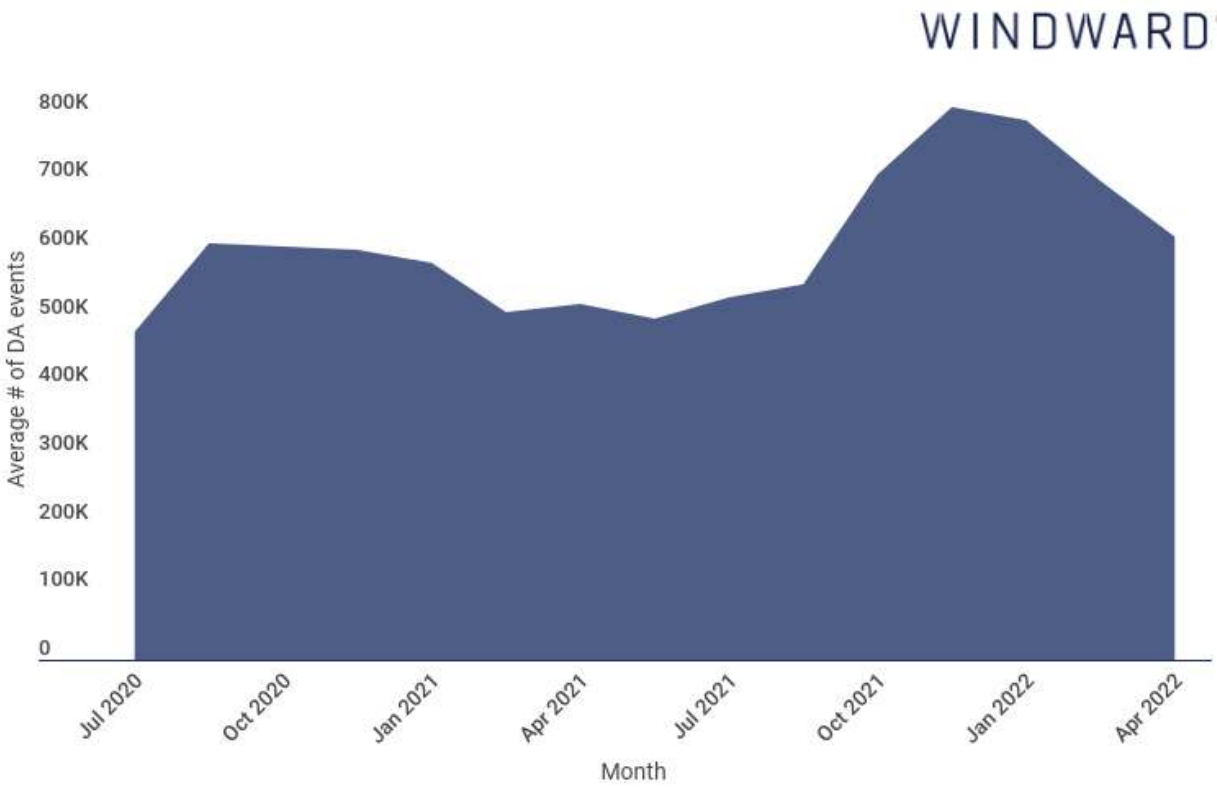

Figure 5: Average number of dark activity events per month (summer of 2020-April 2022)

Context Counts…

To accurately compare between the new deceptive tactics and a widespread deceptive shipping practice such as dark activity, we must first provide the right context. There are hundreds of thousands of dark activities taking place on a monthly basis, so Windward has normalized both trends by dividing the monthly value by the maximal value. In less than a year, location tampering and other emerging trends caught up to the most recurring deceptive shipping practice, dark activity.

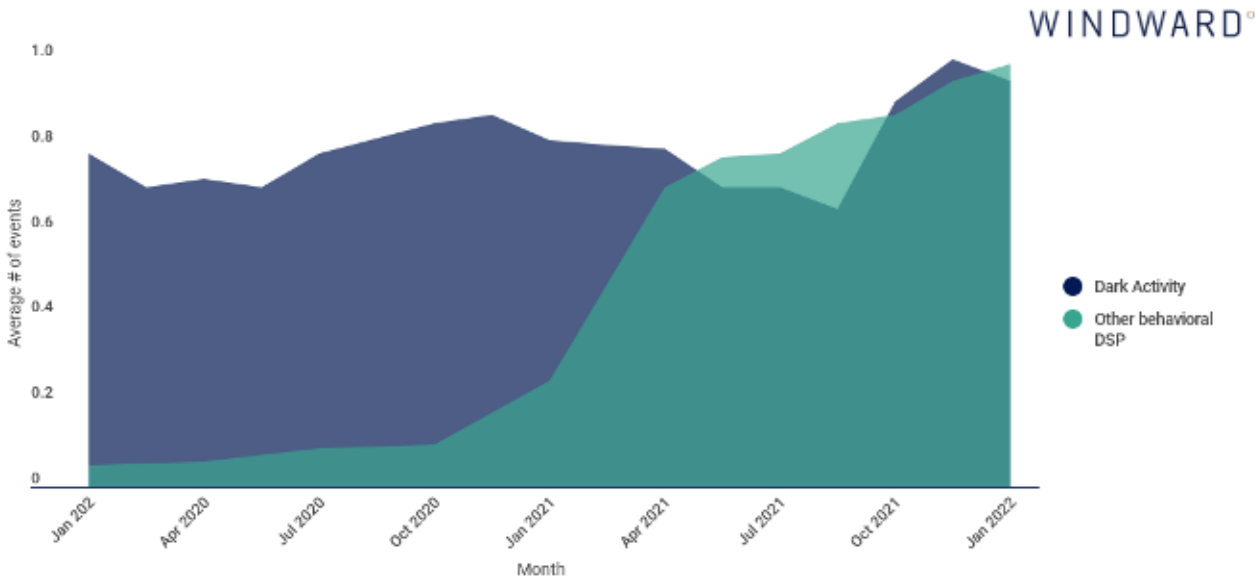

Figure 6: Comparison between dark activity (DA) and other behavioral DSPs

To get an even more laser-focused look into these behaviors, we examined the normalized comparison in a more constrained context, sanctions evasion. The data is compelling. While the exponential growth of location tampering and other behavioral tactics continues at the same rate, dark activity has actually declined, showing it is becoming less popular among vessels transporting sanctioned commodities.

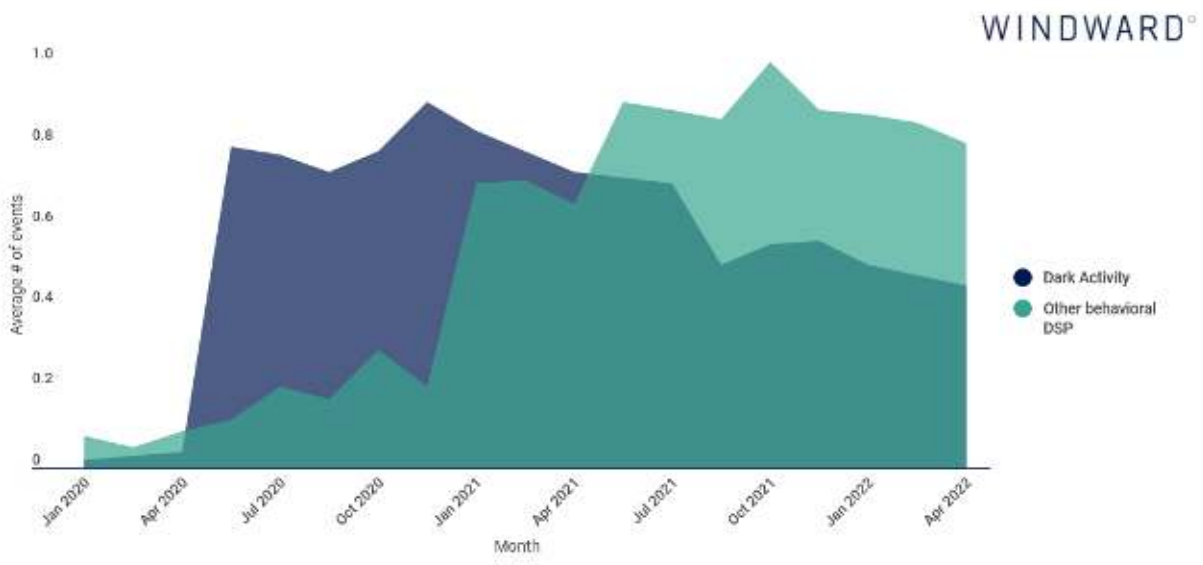

Figure 7: 14-month comparison between dark activity (DA) and advanced DSPs in the context of sanctions evasions

Staying Ahead During a Game of Cat and Mouse

In addition to the insights and research presented in this white paper, multiple articles and research papers have recently explained how deceptive shipping practices are evolving faster than ever. These new tactics allow illicit actors to essentially hide in plain sight and achieve their objectives, without risking their crew or vessel's reputation.

It has become understood in the maritime domain that turning off the AIS transmitter is an immediate red flag detectable by nearly every maritime domain awareness system in the market. At first glance, it seems like dark activity is keeping a steady growth rate, unless data is positioned in the right context.

It's also important to note that trying to detect dark activity without the proper maritime detection technology will lead to endless false positives that will waste your resources (financial and human). By combining vessels'/crews' intent, domain expertise and Maritime AI™ technology, Windward can quickly flag the activities that are worth investigating. Our Dark Activity Insights capability goes beyond accurate differentiation of dark activity from "lost and found"/legitimate transmission gaps. Windward also provides AI-based predictions on the vessel's likely destination, while the vessel is dark.

Bad actors will not stop trying to innovate during this game of cat and mouse, because the potential rewards of illegal activities, such as crude oil smuggling, are obviously high. Without the right technology, legitimate shipping stakeholders (coast guards, government agencies, shipowners, traders, etc.) don't stand a chance. As mentioned in the intro, OFAC is trying to tighten restrictions on Russian oil, but this plan can only succeed if players throughout the maritime ecosystem can identify deceptive shipping practices and refrain from engaging in business transactions with illicit actors. With criminal networks hiding in plain sight, now is the time to invest in a spotlight.

Real-Life Case Studies

Windward utilized our industry-leading technology to detect, track and analyze the pathways and behaviors of real-life vessels engaged in illicit behaviors. This section of the white paper illustrates how rampant the emerging deceptive shipping practices have become. We identified a vessel that engaged in three location tampering incidents within the same year, a vessel that became a zombie vessel, and two vessels engaged in an AIS handshake!

Location Tampering

In June 2020, an 183-meter, Liberia-flagged oil products tanker that previously operated mainly in the Gulf of Mexico changed its ownership and transmitted name. Under its new name, the vessel began operating a shipping line between the Gulf countries and China.

Windward's platform has identified three unique location tampering events in the Gulf area since the vessel began operating under its new name, a behavior firmly connected with sanctions evasion and the trade of illicit cargo.

Chain of Events

Windward tracked a vessel at the Fujairah port waiting area in the United Arab Emirates (UAE) on **February 7**, prior to its journey north. Prominent features of the vessel include: length (180-190 meters), white bridge, red deck, and a white pole at the bow.

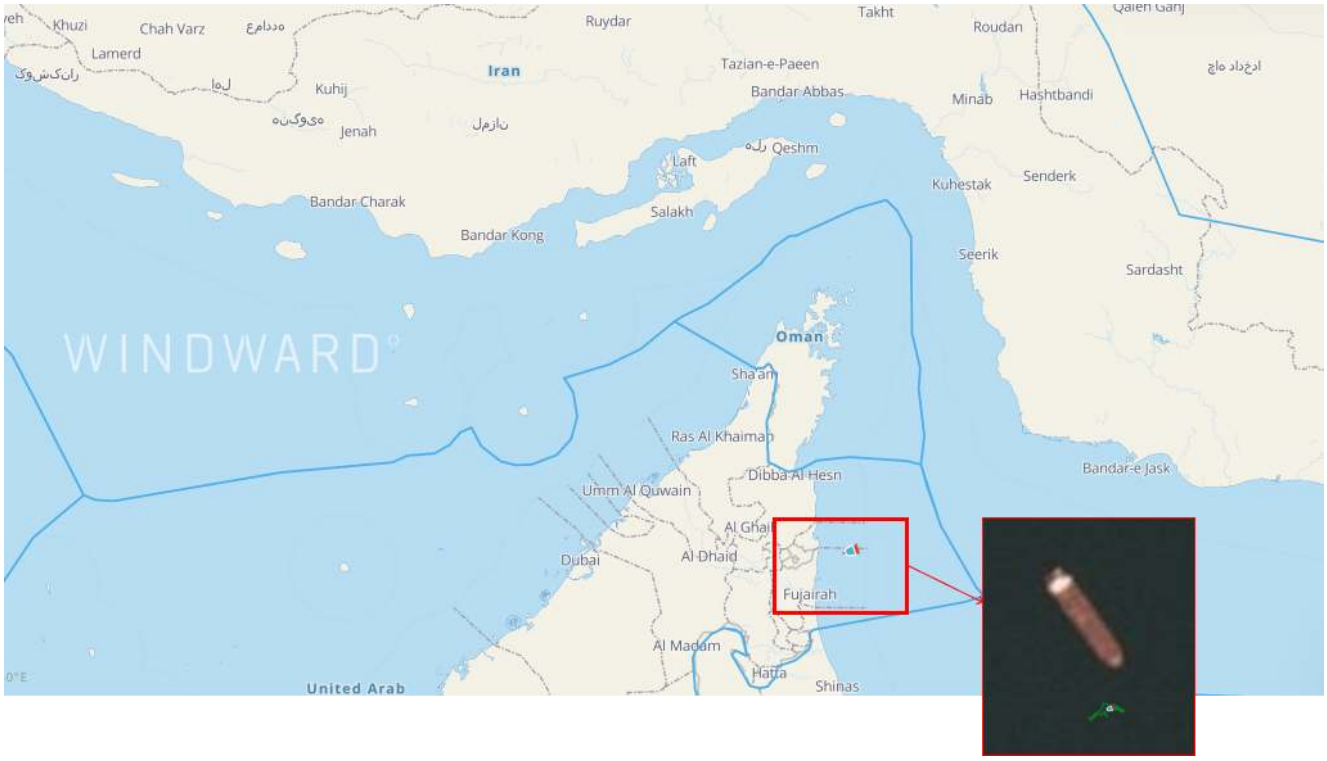

Image 8: The vessels location and satellite image

Following its departure from Fujairah, the tanker sailed towards Iraq and was spotted on **February 14** slowing down just 20 NM away from the Basrah oil terminal. On that same day, **February 14**, the vessel began exhibiting strange, unnatural drifting patterns in the same location outside the terminal, indicating the crew was manipulating its global navigation system.

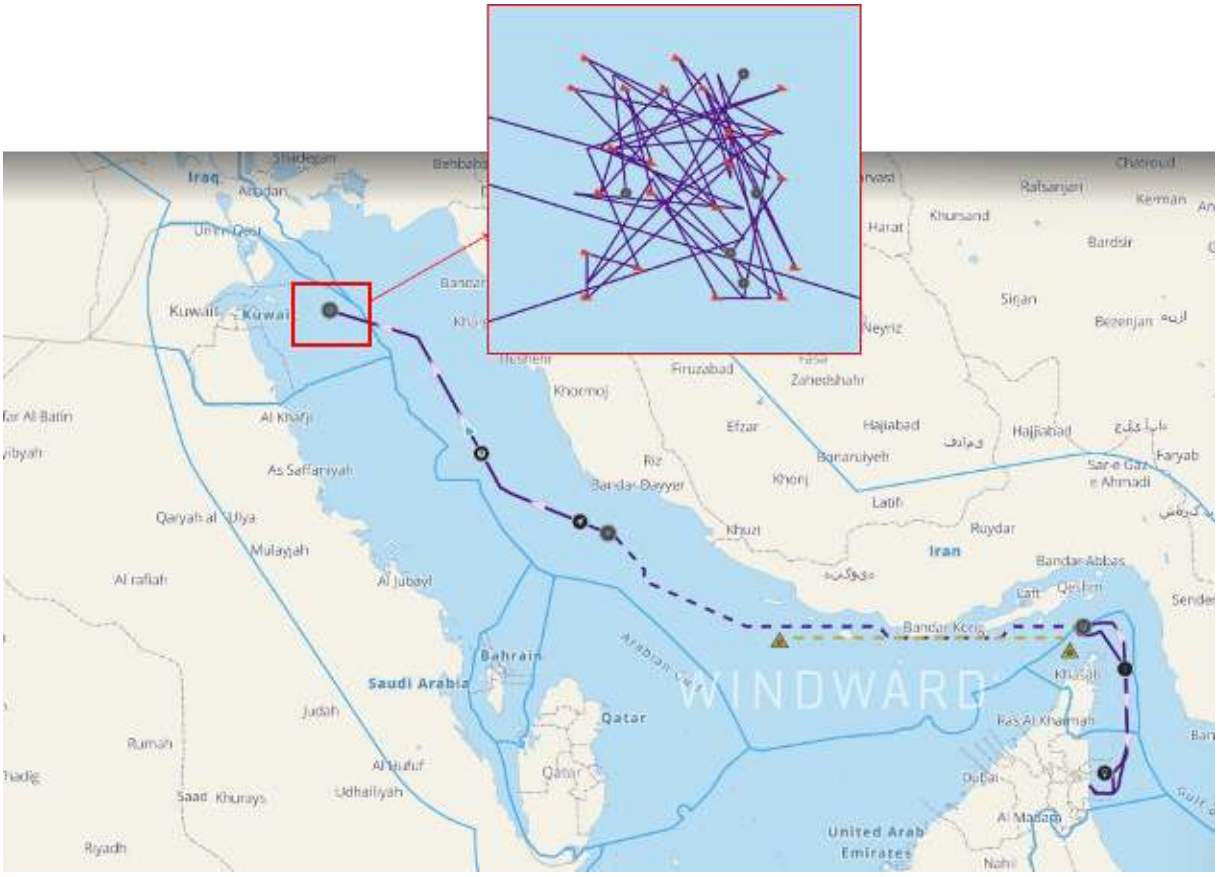

Image 9: Unnatural drifting patterns indicate GNSS manipulation

A satellite image from **February 19** indicates the vessel was not where it is claiming to transmit from. In comparison, another vessel of a similar size just five nautical miles away can be seen in the satellite image, proving the AIS/satellite image matching to be precise.

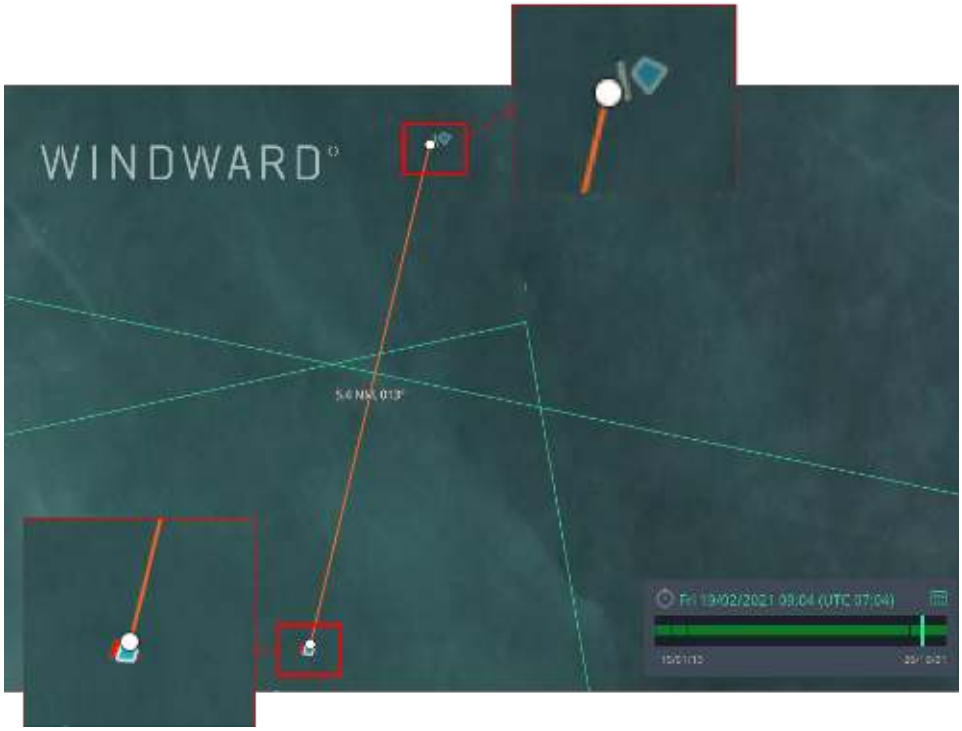

Image 10: Satellite image showing the vessel is not where it's transmitting from

On **February 23**, during the manipulation period, Windward was able to spot a vessel in Kharg Island, one of the main loading terminals in Iran, just 73 NM away from the transmitted location of our vessel. This non-transmitting vessel appeared to be loading at one of the berths and matched our vessel's prominent visual features:

- Length (180-190 meters)
- White bridge
- Red deck
- White pole at the bow

Image 11: Satellite image exposes the non-transmitting vessel loading at one of the berths

On **February 26,** the tanker resumed transmission, heading back towards the Hormuz straits at normal sailing speed, sailing through Iranian territorial waters. The vessel's location upon resuming transmission correlated with the average speed, distance, and time it would take to make the trip back from Kharg Island.

Two days later, on **February 28,** the vessel indicated a change in draft, showing it is fully laden, although there is no activity related to cargo loading, such as a port call or ship-to-ship operation.

Image 12: The transmitted change in draft

Zombie Vessel

Windward also identified another behavioral trend that is growing at an alarming pace – **zombie vessels**. This is a term recently coined by Windward for vessels that use the identity of scrapped ships – essentially resurrecting them from the dead after months or even years of being out of service (and in some cases, literally decimated at scrap yards).

On **April 21, 2022**, a Marshall Islands-flagged tanker arrived at the Alang scrapyard on what appeared to be its final journey. Little did it know, it would be resurrected less than two months later…

Image 13: The vessel in Alang scrapyard on April 21, 2022

On **June 8**, our scrapped vessel sprang back to life and appeared to ”meet” with a tanker known for conducting illicit operations and evading sanctions. However, satellite imagery clearly indicates that only one vessel was physically present at that meeting.

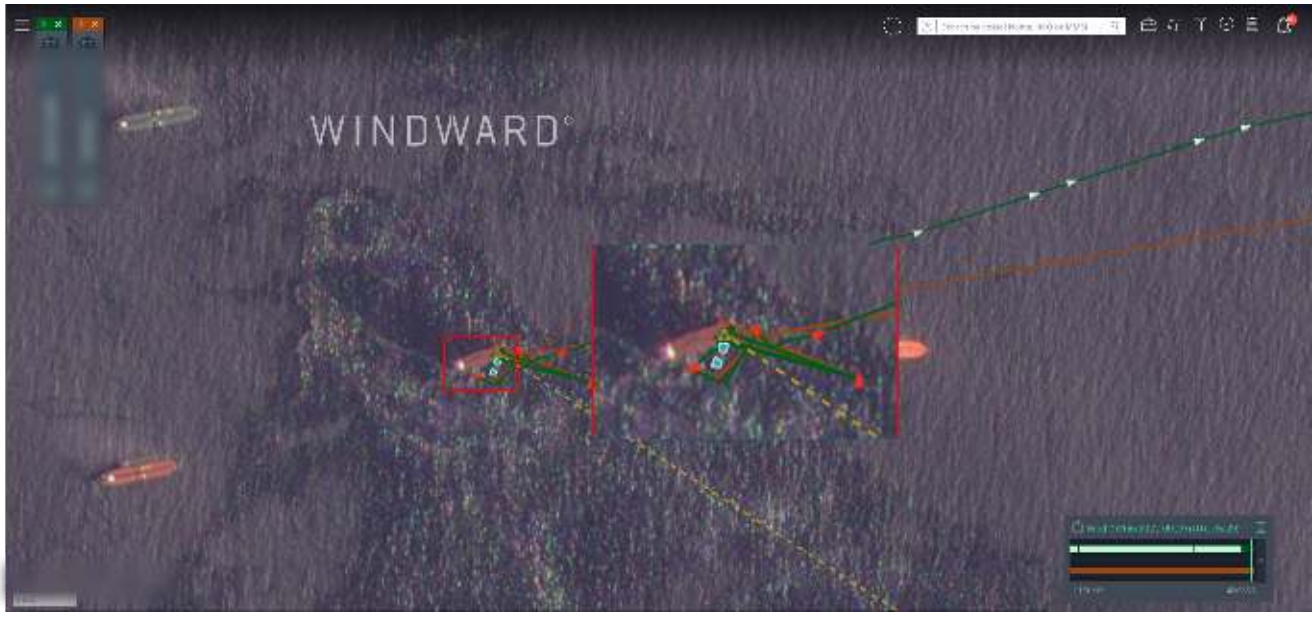

Image 14: Satellite image of the meeting shows two AIS transmissions, but only one present vessel

It was during that “meeting” that our original suspect assumed the “clean” identity of the scrapped vessel and started its new life with a clean slate, as a zombie vessel.

AIS Handshake

On April 26, 2020, the Giessel, a 333-meter crude vessel was sailing under the flag of Saint Kitts and Nevis at the time of this event. The vessel was spotted near Khor Fakkan and reported an empty draft. Three days later, that same vessel had a small positional jump of 2 NM, and suddenly appeared to be transmitting with a whole different ship length (275 meters).

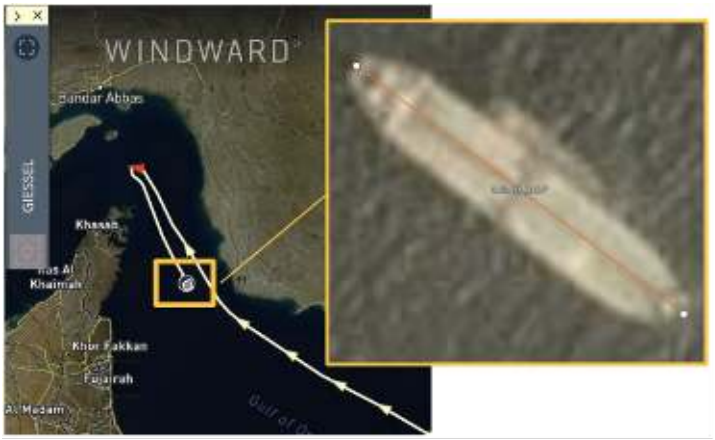

Image 15: The Giessel (left) on April 26, detected via satellite with a 333-meter length near Khor Fakkan. The Giessel (right) detected three days later with a different length (275 meters)

During the time the 275m vessel assumed Giessel's identity, the original 333m vessel was presumably loading Iranian crude oil. It then resumed transmission with a full draft, and its original 333-meter length on May 5, 2020, without any reported loading activity (such as a port call or STS operation). As seen below from the Windward system, the geographic proximity makes this identity handshake even harder to detect for traditional marine domain awareness (MDA) systems.

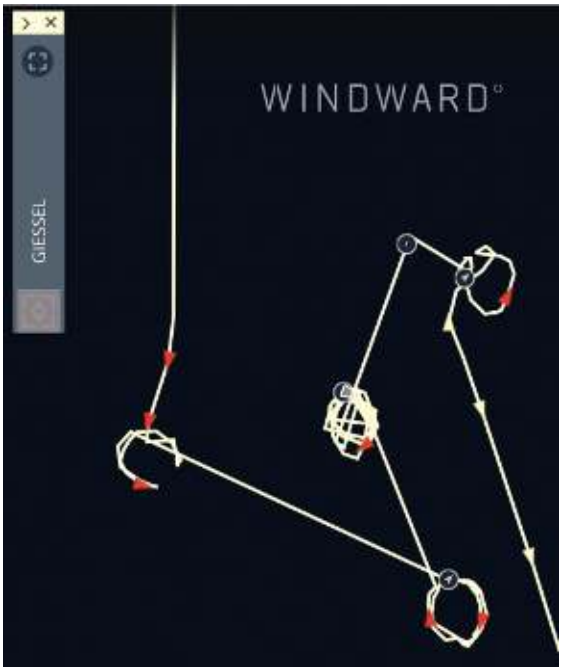

Image 16: The two vessels transmitting near each other before their AIS handshake

Conclusion

Until now, it has been commonly believed that:

- Non-transmitting vessels = bad actors
- Transmitting vessels = safe ships to work with

With OFAC's early guidance as the latest alarm, the industry needs to quickly awaken to the idea that things are a lot more complicated than they seem. It's nowhere near as simple as merely screening for sanctions lists, or detecting dark activity – although that is still relevant and necessary. The cat and mouse game continues to evolve at warp speed, with ships being seemingly resurrected from the dead and complicated ID tampering schemes.

To find and expose the hiders, and mitigate the damage they can cause, government agencies, traders, shipowners, and coast guards will need to quickly understand circumstances and contexts, via maritime expertise and an innovative artificial intelligence system that can automatically flag illicit activities and quickly determine what is actionable.

Windward can help! Contact us.