WINDWARD

AIS Data on the High Seas:

An Analysis of the Magnitude and Implications of Growing Data Manipulation at Sea

Disclaimer

This report was prepared with available data for informational purposes. While Windward has made efforts to confirm such data, it is otherwise provided "As-Is" without representation or warranty of any kind. Windward disclaims any implied or statutory warranties, including without limitation any implied or statutory warranty of merchantability, fitness for a particular purpose or infringement. Windward shall not have any liability for any decisions made on the basis of the report or the data therein.

Executive Summary

AIS data, used routinely by decision makers across industries, is widely perceived as a reliable source of information on ship activity worldwide. Massive financial investments and critical operational Decisions are based on this data.

New research from Windward reveals that AIS data has critical vulnerabilities when used to track ships, an 'off label' use of the system. The data is increasingly manipulated by ships that seek to conceal their identity, location or destination for economic gain or to sail under the security radar.

Manipulation practices are varied, according to our research, and range from Identity Fraud, to Obscuring Destinations, 'Going Dark,' Manipulating GPS, and 'Spoofing' AIS. Ships that manipulate AIS undermine not only their own data, but the entire maritime global picture -- once some of the data is corrupt, all data is suspect.

Worldwide Ship Activity: One of the Last 'Wild West' Frontiers

Shipping activity across the world's oceans is the lifeblood of the global economy, transporting billions of tons of goods annually and facilitating global commodity flows of oil, coal, grains and metals. Vessel activity is also of critical importance to Intelligence and Security agencies worldwide, as criminal and terrorist activity has become increasingly global and borderless.

And yet, the oceans remain one of the last 'wild west' frontiers, with limited visibility on what ships are actually doing once they leave port. AIS data, the most widely used data on ship activity worldwide, underlies decisions from Finance to Intelligence, but the data is unreliable and increasingly manipulated by the very ships it seeks to track. And this trend is growing, fast, with little-understood and far-reaching implications worldwide.

AIS data has become industry benchmark but is increasingly manipulated

AIS data, used across industries, has critical vulnerabilities: it is increasingly manipulated by ships that seek to conceal their identity, location or destination for economic gain or to sail under the security radar.

'Off Label' Use of AIS: Data Danger Zone

Until very recently, ships literally disappeared once they sailed past the horizon, resulting in a complete information vacuum for anyone interested in tracking ship activity. In 2002, the International Maritime Organization (IMO), a U.N. agency, began mandating that ships above a certain size, as well as all tankers and passenger ships, transmit their information to nearby ships and onshore receiving base stations in order to avoid collisions and promote maritime safety.

Commercial satellites revolutionized the industry in 2008, picking up the same AIS transmissions from space and providing visibility on ships offshore for the first time in history. Today, ships transmit well over 100 million data points per day, known as AIS data, collected by satellites and networks of coastal receivers and sold to anyone interested in tracking ships at sea.

However, this 'off label' use of AIS – for tracking ships– has hugely significant but little-understood implications. Because AIS was designed to promote safety, it is a publicly available data stream with weak security mechanisms.

Further undermining the quality of the data, there are no information assurance mechanisms in place to ensure that ship transmissions are, indeed, accurate. As a result, while ships are required to transmit information, there are myriad ways to conceal a ship's identity and destination and the satellites that receive the data have no way of validating the accuracy of the information.

New Findings

New research from Windward sheds light, for the first time, on real-world AIS manipulation, the magnitude of the problem and its implications, especially for Finance and Intelligence constituents.

The research is based on aggregated shipping data from publicly available sources, looking at data on all AIS-fitted ships worldwide, estimated at over 200,000 vessels, from July 2012 through August 2014.

The overarching finding of this research, discussed in more detail below, is that AIS data has massive vulnerabilities when used for tracking ships, and that these vulnerabilities are being increasingly exploited by ships (i.e., interested parties) intent on concealing their identity, destination or activities.

Top Five AIS Manipulation Practices

New research by Windward identifies the top AIS manipulation tactics:

- *Identity Fraud*
- *Obscuring Destinations*
- *'Going Dark'*
- *GPS Manipulation*
- *AIS Spoofing*

The vulnerabilities come in several 'flavors' – Identity Fraud, Obscuring Destinations, 'Going Dark,' GPS Manipulation, and Spoofing AIS - but all share a single goal: distorting the maritime picture and with it the ability of decision makers to act on valid, reliable data. The implications of relying on this increasingly manipulated data are, as discussed below, vast and far reaching.

Our research focused on the 'top five' manipulation practices currently being used around the world:

Identity Fraud

Findings: Ships are increasingly transmitting false or stolen identifying marks, taking advantage of the AIS 'honors system,' as ships are required to transmit their information but there is no way to validate that data. This phenomenon is widespread, with 1% of all ships using fake identification information (called 'IMO numbers') over the past year, resulting in several hundred vessels 'in disguise' at any given time. This is akin to having over 1000 people going through John F. Kennedy International Airport each day using fake IDs.

Impact: Anyone tracking a ship via AIS data, whether a security organization or a New York-based hedge fund, has no assurance that the name on the screen does, in fact, correspond to the physical ship of interest. This rising trend poses a significant threat to maritime security.

Obscuring Destinations

Findings: Vessels do not report their next port of call more than half of the time. In fact, in our research, the final port of call was reported by ships, on average, only 41% of the time.

Impact: For anyone tracking global commodity flows – where commodities are heading, when they are expected to arrive – the missing final port data doesn't just create an information gap, it could well be intentionally misleading, skewing the view of global commodity flows.

'Going Dark'

Findings: The most commonly-seen manipulation practice is vessels turning off their AIS transmissions, with over one quarter of the vessels worldwide turning off their AIS at least 10% of the time, taking into account active shut downs vs. lack of satellite coverage.

Large vessels (over 250m) are more likely than others to turn off their transmissions, suggesting that vessels engaged in global trade, and carrying the most significant amounts of cargo, have greater incentive to conceal their activities at certain times.

Impact: The simplicity of turning off AIS – similar to separating a battery from its cellphone to avoid tracking - is a challenge for both financial and security stakeholders, as it severely undermines their ability to track vessels and monitor areas.

GPS Manipulation

Findings: AIS transmitters do not provide GPS validation. Therefore, whatever positioning data is 'fed' into the device is transmitted as the vessel's position, regardless of the ship's actual position. Within just the last year, from mid-2013 to mid-2014, there has been a 59% increase in the use of GPS manipulation.

Impact: Tampering with the GPS feed of AIS is a growing and concerning practice, likely to further evolve over time. It allows ships to suddenly 'reappear' in other parts of the world – similar to a plane flying over Miami manipulating its GPS so that it appears to air traffic control and other parties to be flying over Seattle - making it extremely difficult to know a vessel's actual whereabouts.

Spoofing AIS

Findings: As previously shown in important research by Dr. Marco Balduzzi and his team at Trend Micro, AIS can be 'spoofed' and inserted into the data stream, allowing people to create 'ghost ships' where none exist.

Impact: If 'ghost ships' are created, these false entities can negatively impact the maritime situational picture, particularly in areas of conflict.

Taken together, these findings paint a troubling picture of the scope and magnitude of this growing trend, with implications for both intelligence and business organizations worldwide.

Incentives and Implications – Shipping and Finance

Shipping and trading have been traditionally opaque markets, with little public data available. And global commodity flows over the oceans have huge economic value: Global crude imports in 2013 were over $2,823B, with half transported by sea. The financial trading on this volume is estimated by the EIA to be nine times larger than the transport value. Total coal export sales in 2012 amounted to $128.692 billion, with approximately 98% shipped by sea. Total exported iron ore sales in 2012 were $125.474B, the majority shipped by sea.

As such, the introduction of AIS data holds huge potential for traders, informing both micro-level analysis - what a given ship is carrying and where it is headed – and the evaluation of macro-level trends, such as the expected oil supply for a certain country or imports and predicted growth in specific regions.

Implications for Finance:

For commodity traders, hedge funds and others tracking global commodity flows, basing decisions on AIS data has vast implications:

- *Distorted View of Commodity Flows*
- *Flawed Understanding of Supply and Demand*
- *Impact on Trading Models*

However, the economic incentives for various players to intentionally obscure the picture by manipulating AIS data are vast, as any edge, fundamental or tactical, can potentially have tremendous economic value.

Trading decisions are only as good as the data they rely on, and this axiom is particularly true for trading based on data-driven models and quantitative analysis, which require a high level of data reliability. Valid AIS data gives traders a strong, reliable foundation for their trading strategies; conversely, invalid, intentionally manipulated data can have a significantly negative impact on trading decisions and outcomes.

AIS manipulation has three main implications for the Finance world:

Distorted View of Commodity Flows

Understanding commodity flows is directly linked to knowing the actual movement of ships, and flawed AIS data can create an inaccurate and misleading analysis of key metrics, such as how much of a given cargo is being transported by sea.

Flawed Understanding of Supply and Demand

Freighting rates are determined by the supply and demand in specific ports and areas. Knowing how many ships are open in a specific port or which cargo has left port is extremely valuable information. AIS data that is able to 'hide' ships or cargoes and obscure destinations can have tremendous economic impact by affecting the perception of supply and demand.

Impact on Trading Models

Trading models that are data dependent are designed to account for expected data deviations. However, because AIS data is being manipulated and there is no validation mechanism in place to control the phenomenon, there is no way of knowing the actual scope of the false data and adjust models accordingly. In addition, the method of 'counting ships,' prevalent to date as a way to gauge cargo and commodity flows, is increasingly unreliable. As companies build bigger ships with greater cargo capacity in order to increase efficiency, the potential impact of missing any single ship is getting more and more significant.

Incentives and Implications – Security and Law Enforcement

In just a decade, AIS has gained a pivotal role in the day-to-day operations of many security and law enforcement agencies, from Navies to Coast Guards to Customs and Intelligence agencies. Today, AIS data is integrated into many national systems for controlling and enforcing laws in their exclusive economic zones, enhancing Maritime Domain Awareness and promoting safety at sea.

But AIS manipulation has a tremendous impact on governmental agencies, as it obscures some of the key activities they seek to monitor including smuggling, terrorism, immigration, sanction violation, illegal fishing, oil bunkering, safety issues and even militarized conflicts. For agencies tracking these activities, the challenge is identifying specific ships of interest while continuously monitoring large sea areas in real time to respond to emerging threats.

Implications for Security:

Security agencies face alarming consequences when relying on AIS data:

- *Trust No One*
- *Beware of Ghost Ships*
- *Erasing Digital Footprints*
- *Undermining Watch Lists*

There are four main implications for security and law enforcement:

Trust No One

AIS data cannot be trusted 'as is' as it is increasingly manipulated by the very parties security and law enforcement agencies seek to monitor. Once some of the data is flawed, none of it can be trusted. Effectively using AIS for maritime control and security requires the ability to continuously vet vessel transmissions in order to identify the 'bad guys'.

Ghost Ships

AIS can be manipulated to insert fake ships into a country's maritime situational picture. For example, hackers can make military vessels 'appear' near a sensitive region, potentially heating up a border and elevating geopolitical tensions.

Erasing Digital Footprints

Ships are able to actively erase their digital footprints, removing evidence of the ship's activities, and even leave a false evidence trail. Efforts to monitor a given area are severely damaged when valid information on a ship is non-existent or intentionally misleading.

Undermining Watch Lists

Watch lists are one of the most common tools of maritime security and law enforcement, enabling authorities to be on the lookout for specific vessels of interest, cargoes and crew members based on prior intelligence. By concealing identities and activities, the effectiveness of watch lists decreases dramatically.

AIS Manipulators: The Early Adopters

Another significant concern is the overall growth of AIS manipulation. Today's AIS manipulators are the 'early adopters' of a tactic for gaming the system. Some of the early adopters may include Chinese fishing vessels engaged in illegal fishing, large shipping companies seeking to maintain market opaqueness, oil tankers circumventing international sanctions, and large oil producers concealing oil via floating storage in

order to affect global oil prices. This group will likely be followed by far more ships seeking to conceal their information in the future.

This growing trend is likely a direct reaction to ships' growing awareness that they are being 'watched' via AIS transmissions and the incentive on the part of some players to preserve opaqueness by misreporting.

Small Numbers with an Outsized Influence

While AIS manipulation is on the rise, most AIS data is accurate. However, the relatively small group of AIS manipulators have an oversized impact, since they are likely the very ships (people) that have the incentive to manipulate the data.

Game of Chance

Looking forward, perhaps the greatest implication of these findings is that AIS is becoming a 'Game of Chance,' with players making major decisions based on data they believe is accurate, while the reality is that this data – particularly the 'interesting' data – is, and will increasingly be, influenced by players with conflicting interests.

Game of Chance

Once SOME AIS data is intentionally manipulated, ALL AIS data becomes suspect, making the use of this data at 'face value' a costly, or dangerous, Game of Chance

Conclusion – AIS Cybersecurity

Decisions are only as good as the data they rely on. AIS manipulation is a fast-growing, global trend undermining decision makers who rely, unknowingly and unwittingly, on inaccurate and increasingly manipulated data.

As regulation increases, we expect to see ever-growing amounts of AIS data, with ever declining quality, as ships become aware that they are being 'watched' via their AIS transmissions and employ the varied mechanisms discussed above, and others that will surely come to light, to avoid detection. We can no longer afford to take AIS at 'face value.'

In 2008, satellites revolutionized the industry and provided visibility on ships off shore for the first time in history. It is now time to again employ technology to make sense of this data and ensure that it is a reliable, valid source of information for decision makers worldwide. It is time to employ AIS Cybersecurity countermeasures to stop AIS from becoming a game of chance.