Journal of *Marine Science and Engineering*

MDPI

Article

AIS Data Manipulation in the Illicit Global Oil Trade

Andrej Androjna [1], Ivica Pavić [2], Lucjan Gucma [3], Peter Vidmar [1] and Marko Perkovič [1,*]

[1] Maritime Department, Faculty of Maritime Studies and Transport Portorož, University of Ljubljana, 6320 Portorož, Slovenia; andrej.androjna@fpp.uni-lj.si (A.A.); peter.vidmar@fpp.uni-lj.si (P.V.)
[2] Maritime Department, Faculty of Maritime Studies Split, University of Split, 21000 Split, Croatia; ipavic71@pfst.hr
[3] Department of Marine Traffic Engineering, Maritime University of Szczecin, 70-500 Szczecin, Poland; l.gucma@am.szczecin.pl
* Correspondence: marko.perkovic@fpp.uni-lj.si

Abstract: This article takes a close look at the landscape of global navigation satellite system (GNSS) spoofing. It is well known that automated identification system (AIS) spoofing can be used for electronic warfare to conceal military activities in sensitive sea areas; however, recent events suggest that there is a similar interest of spoofing AIS signals for commercial purposes. The shipping industry is currently experiencing an unprecedented period of deceptive practices by tanker operators seeking to evade sanctions. Last year's announcement of a price cap on Russian crude oil and a new ban on Western companies insuring Russian cargoes is setting the stage for an increase in illegal activity. Our research team identified and documented the AIS position falsification by tankers transporting Russian crude oil in closed ship-to-ship (STS) oil transfers. The identification of the falsified positions is based on the repeated instances of discrepancies between AIS location suggestions and satellite radar imagery indications. Using the data methods at our disposal, we reconstructed the true movements of certain tankers and encountered some surprising behavior. These false ship positions make it clear that we need effective tools and strategies to ensure the reliability and robustness of AISs.

Keywords: automatic identification system (AIS); tankers; falsification; spoofing and jamming

Citation: Androjna, A.; Pavić, I.; Gucma, L.; Vidmar, P.; Perkovič, M. AIS Data Manipulation in the Illicit Global Oil Trade. *J. Mar. Sci. Eng.* **2024**, *12*, 6. https://doi.org/10.3390/jmse12010006

Academic Editor: Dejan Brkić

Received: 19 November 2023
Revised: 9 December 2023
Accepted: 12 December 2023
Published: 19 December 2023

1. Introduction

In spite of the ban on imports of Russian crude oil and products and the ban on ships calling at certain ports, a number of shipping companies are supporting Russian exporters. While it must be recognized that there is a fundamental clash between nations and industries, the growing ghost fleet of substandard ships carrying sanctioned Russian goods around the world's seas is certainly a danger at sea: many of these vessels are not seaworthy, operate with incompetent crews, and have already been involved in enough accidents to raise some degree of alarm. All of this is possible because the bans on imports of Russian crude oil and ships entering certain ports apply only to certain countries [1,2]. Yet, some shipping companies can continue to transport Russian oil without facing consequences as a ghost fleet of unregistered vessels (that do not officially exist) is growing, and it is difficult to track down such vessels. The ghost fleet can transport these goods undetected because they are not registered with any country's maritime authority and are not subject to any regulations or inspections. These vessels undermine the effectiveness of sanctions by allowing sanctioned goods to travel around the world undetected. They also pose a security risk to global shipping, given the lack of inspections. Finally, they create an environment in which illegal activities, such as smuggling, can flourish. Addressing these risks requires coordinated efforts by governments and international organizations. For now, we must set aside the debate over the logic and efficacy of sanctions themselves. One approach is to increase the surveillance and monitoring of maritime activities to detect suspicious vessels.

Another is to impose stricter regulations on shipping companies and force them to provide more detailed information about their vessels and cargoes. In addition, countries can work together to enforce sanctions more effectively by sharing information and coordinating their efforts.

It should be noted that cargo transfers do not occur in ports, but at sea, either at an anchorage outside territorial waters where the water depth permits this, or further out at sea where ships either drift with the current and wind or move slowly, engaging in a process called ship-to-ship transfer (STS transfer), which is commonly used in the shipping industry to transfer large quantities of oil or other cargo between vessels. STS transfers can be performed using a variety of methods, including hoses, pipelines, and pumps [3,4]. However, if performed improperly, this process poses risks, such as oil spills and accidents. As a result, strict regulations and safety protocols are in place to ensure that such transfers are conducted safely and efficiently, and this is even more important as the demands for oil and other commodities continue to grow and STS transfers are likely to continue to play an important role in moving goods around the world.

Most commonly, STS operations are used to handle crude oil, petroleum products, and liquified gas [5]. The STS operations of the International Convention for the Prevention of Pollution from Ships (MARPOL) Annex I's cargo within territorial waters (TTWs) and the exclusive economic zone (EEZ) of a MARPOL Contracting Party are reported in advance to the competent authority of the coastal state, while coastal state authorities may require notifications for MARPOL Annex II and other cargoes. All other issues are subject to local regulations [6]. STS transfers require careful planning and coordination to ensure the safety of the vessels involved and to prevent oil spills, accidents, or damage to the ships or cargo. Planning considers factors, such as the limits of the transfer area, environmental constraints, weather conditions, sea state, traffic density, good holding conditions, ships' characteristics, and compliance with international and local regulations [7–9].

This operation requires compliance with various legal and technical requirements established by the International Maritime Organization (IMO) and other relevant organizations. IMO Resolution MEPC 186(59)/2009 amended the MARPOL Annex I by adding Chapter 8 to provide a common international framework addressing applications, preparations of STS operation plans, persons in overall advisory control, retention of records on board, and notifications for operations within the TTW and EEZ [8]. In addition, the publication Ship to Ship Transfer Guide for Petroleum, Chemicals and Liquefied Gasses, developed by maritime industry organizations, provides guidance and recommendations for the planning and actions of all responsible persons involved in the operation [5].

Since it is a complex operation that can lead to accidents at sea, it is necessary to conduct a safety and risk assessment. Ventikos and Stavrou [4] described some recent developments, including the identification of risk factors and their roles in risk assessments. They applied a fuzzy inference system (FIS) for the risk assessment [9] and a process failure mode and effects analysis (PFMEA) in combination with FIS methodology to assess and evaluate risk scenarios of STS transfer operations [10]. Sultana et al. conducted a comparative analysis between a system theoretical process analysis (STPA) and hazard and operability studies (HAZOP) for liquefied natural gas (LNG) STS transfer systems and concluded that the STPA technique provided effective systematic guidance and recommendations for safety requirements [11]. These studies demonstrate the importance of risk assessments for STS operations.

Depending on the legal basis, STS transfer can be divided into two categories: legitimate and illicit. Legitimate transfer is an operation conducted in accordance with IMO regulations, technical guidelines of relevant organizations, and national regulations within the framework of regular (legal) maritime trade. In contrast, illicit transfer is conducted to disguise the violation of sanctions or embargoes, smuggle illegal cargo, or, simply, engage in any illegal maritime trade. There are numerous reported cases of sanction violations committed through illicit STS operations [12–15]. In the two piracy hotspots (Southeast Asia and West Africa), illicit STS is also known to have been performed as part of piracy and

armed robbery operations aimed at stealing oil cargoes [16,17]. In recent developments, STS transfer is becoming one of the oil smuggling techniques used worldwide, basically outside the traditional trade routes. The Israeli company (one should always consider potential biases of private company results, given the fraught diplomatic conditions in the world) Windward's Maritime AI^{TM} platform identified four suspicious operational patterns in Russian oil smuggling. These patterns are aimless journey, checkpoint avoidance, floating storage and ID, and location tampering, which allows vessels to disguise their locations and conduct illicit STS operations that usually occur in the mid-North Atlantic [18].

The patterns show the ability to conduct illegal activities to evade sanctions. According to the UK P&I Circular 01/22, there are some techniques used to evade sanctions, such as manipulating AIS data, changing the vessels' physical appearance, falsifying ship and/or cargo documents, and multiple STS operations [15]. Of particular interest to our research is AIS data manipulation used to evade sanctions through illicit STS operations.

Although AIS is not a system for preventing illegal activities at sea, AIS data deviations can be a great help in detecting such activities. Originally, AIS was intended as a communication system to improve the safety of navigation, exchanging navigational and other data between ships and the shore. At present, the data from AISs are not only used for safety of navigation, but also for maritime safety and security purposes, such as vessel tracking; route and fishing activity monitoring; maritime risks and trend analyses; accident investigations; waterway planning; management and maintenance; scientific, environmental, and ecological purposes; and the prevention of illegal fishing, piracy, armed robbery, etc. [19–26]. In connection with the expansion of the use of AIS data, it should be mentioned that research has recently been conducted on the use of AIS data in the area of critical infrastructure protection. Soldi et al. analyzed how information from different sources, in particular, AIS and satellites (i.e., synthetic aperture radar—SAR), could be fused to detect anomalous and suspicious behavior and identify threats to critical underwater infrastructure [27].

The wide application of AIS was adopted because of its advantages. Numerous design-related disadvantages led to AIS vulnerabilities. AIS is an insecure open broadcast system [28] that transmits on two dedicated maritime public VHF frequencies [29]. AIS data are not encrypted and there are no mechanisms to perform authentication, timing, and validity checks [28–30]. Therefore, AIS stations are vulnerable to spoofing, hijacking, and availability disruption [31]. Various solutions have been proposed in the context of improving the protection and integrity of AIS data. In this sense, Iphar et al. described the use and misuse of AIS data and proposed a data integrity assessment method to detect anomalies in AIS messages. They also presented a risk assessment that individualized these messages and evaluated the risk values according to the different message characteristics [32,33]. AIS signal reception is one of the disadvantages that can be exploited in illegal activities. Salmon et al. analyzed the problems with the reception of AIS signals and introduced the concept of black holes for maritime areas where AIS signals could not be received by coastal stations [34]. Malicious actors can manipulate the data from AISs and transmit deceptive or false data [28].

The UK P&I identified three techniques of AIS data manipulation for the purpose of evading sanctions. These techniques are switching off the AIS, GPS/GNSS manipulation, and AIS misuse [15]. Technically, switching off an AIS is the simplest technique. During STS transfer, the AIS is switched off. According to Regulation V/19.2.4.7 of the International Convention for the Safety of Life at Sea (SOLAS), an AIS must be in continuous operation [35], while according to IMO Resolution A.1106(29), switching off an AIS is allowed only when its operation can endanger the safety or security of the ship or when a security incident is imminent [36]. Since STS transfer does not threaten the safety and security of the ship, turning off the AIS is not allowed. It is important to note that the maritime community is making additional efforts to discourage switching off AISs. In this regard, the Baltic and International Maritime Council (BIMCO) have developed an AIS

switch-off clause for time and voyage charter parties that allows shipowners and charterers to terminate contracts with contractors who switch off AISs for improper reasons [37].

In our previous articles [38,39], we scrutinized the landscape of AISs as an important source of information for maritime situational awareness (MSA), highlighting its vulnerabilities, challenges, and cybersecurity in relation to safe navigation and shipping. Complemented by a case study of a specific spoofing event near Elba in December 2019 [39], which confirmed that a typical maritime AIS could easily be spoofed and, in the case of this study of suspicious STS oil transfers, generate a false position or even no position, we confirmed, once again, that AIS messages could be spoofed, disrupted, deliberately faked, or simply shut down.

The paper is structured as follows: Section 2 presents the methodology; Section 3 presents AIS vulnerabilities and results made explicit through case studies. Section 4 presents the discussion and Section 5 the conclusions.

2. Methods

2.1. Automatic Identification System

At present, the easiest way to track ship traffic is through the AIS system, as all large ships are equipped with a radio system that automatically transmits dynamic and static information about the ship. The position of the ship, its speed, and even its rate of turn are transmitted very frequently; a normal ship, while underway transmits at least 6 positions per minute. When maneuvering, the frequency increases by threefold, and when the ship is at anchor or in port, it transmits the data once every three minutes. Although the rate of turn (ROT) is an AIS function, this value is not displayed correctly in some messages, and therefore may only be used sometimes. The data quality is better for large vessels displacing over 50,000 tons, which must be equipped with an ROT indicator that provides more reliable reports on the rate of turn transmitted by the AIS system. A coastal AIS base station can also interrogate the ship's AIS transmitter to speed up the transmission, up to every two seconds, which is especially useful when the ship is maneuvering or when ships at anchor are exposed to bad weather. So, when we track a ship on its course, we generally have a position at least every 72 m (without taking into account the GNSS positioning performance and possible jamming or spoofing activities), and the exact data are given by Equation (1) and Figure 1 presenting a plot of all the ship distances traveled between consecutive measurements.

$$S(\triangle T, V) = V \cdot \frac{1852}{3600} \cdot \Delta T(V) \left\| \begin{array}{c} \Delta T(V) = 10s \; for \; V < 14kn \\ \Delta T(V) = 6s \; for \; 14 \leq V < 23kn \\ \Delta T(V) = 2s \; for \; V \geq 23kn \end{array} \right. \quad (1)$$

where ΔT is the AIS reporting interval and V is the ship's velocity (speed over ground).

Of course, all this is true only if the ship is within the range of a shore base station and if the VHF link operates at a high performance, but this is not always the case. The expectations for integrity, availability, and reliability were unfortunately not met by the AIS developers or could only be explained by its anti-collision short-range nature, where integrity and reliability were not the basic requirements. For VHF propagation, the range depends mainly on the heights of the transmitter and receiver antennas. The expected range between the AIS base station with an antenna 49 m above sea level and the ship station with an antenna height of 25 m (smaller vessels) corresponds to 30 NM according to Equation (2):

$$D = 2.5\left(\sqrt{h_1}\right) + \sqrt{h_2}, \; \mathrm{D} = 2.5\left(\sqrt{49\ m} + \sqrt{25\ m}\right) = 30\ NM \quad (2)$$

Some coastal stations are located on very high hills; so, an AIS base station at an altitude of 1089 m can track a larger ship at a distance of 100 NM, as seen in the following table.

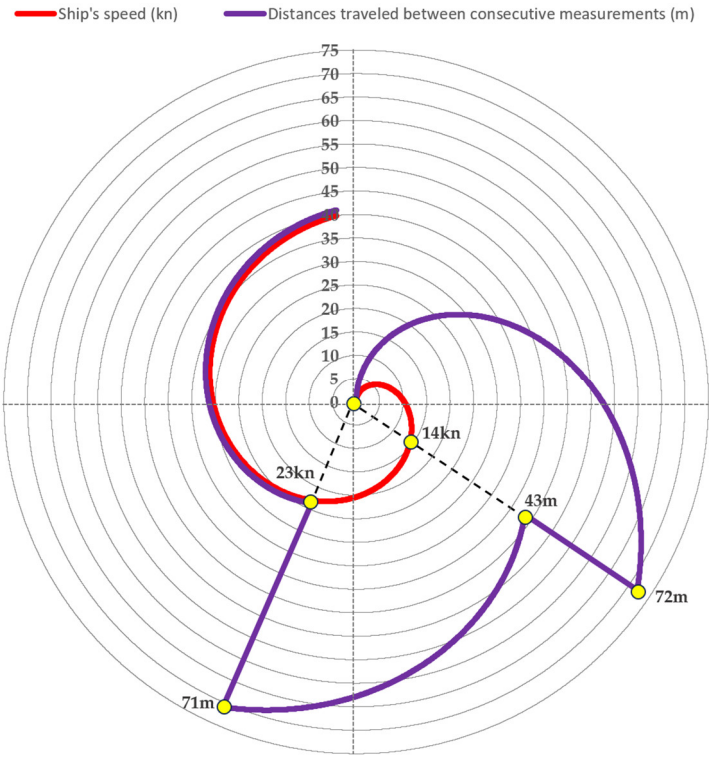


Figure 1. Distances traveled between successive AIS messages.

Occasionally, distances can be much larger due to the effects of atmospheric ducts on AIS propagation [40,41]; these situations should normally be relatively rare, but with the heavy evaporation of the water surface, this is more common over the ocean in summer. A very illustrative picture of the possible atmospheric ducts can be seen in Figure 2, where the range of AIS stations in the Black Sea area is very high. However, considering the relatively low height of all base stations' VHF antennas around Costanța, it is difficult to believe that all stations can receive signals from smaller vessels located in the Sea of Azov.

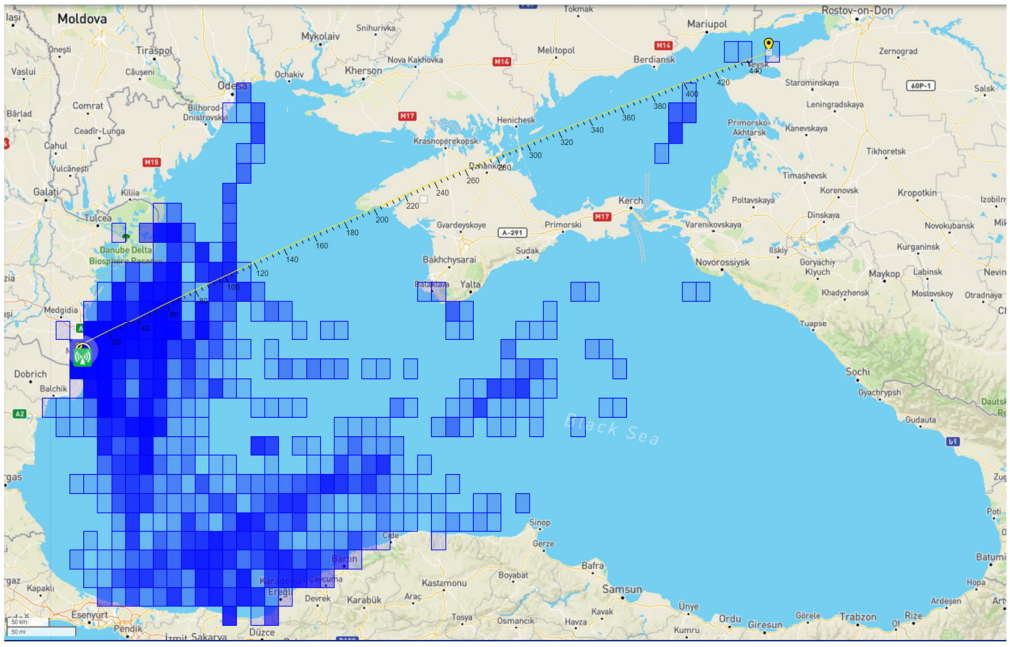


Figure 2. AIS range of Costanța base station (9 March 2023); source: produced from Marine Traffic.

Using the range method from at least two base stations, it was possible to determine the positions of suspect vessels located at distances beyond the range of the terrestrial AIS system.

An example of an exceptional AIS range is shown in the following figure, depicting the average and maximum receiving distances of three AIS stations during the period from October 2022 to 2023. All three stations are located near Costanța at similar altitudes, namely, Costanța Station (h = 41 m), Constanta Kalimbassieris Maritime Station (h = 20 m), and Offshore Costanța Station (h = 10 m). Figure 3 shows the extreme range of the AIS system on 9 March 2023, when it exceeds 450 nautical miles. One can speak of atmospheric disturbances, but other stations in the western part of the Black Sea do not have such a range. Nor can one imagine special conditions in March, known as the time of the summer solstice. All three stations are located at low altitudes; their realistic range, according to Table 1, is not more than 40 NM, even for communication with a large merchant ship, where the AIS antenna can be placed at a height of 60 m above sea level.

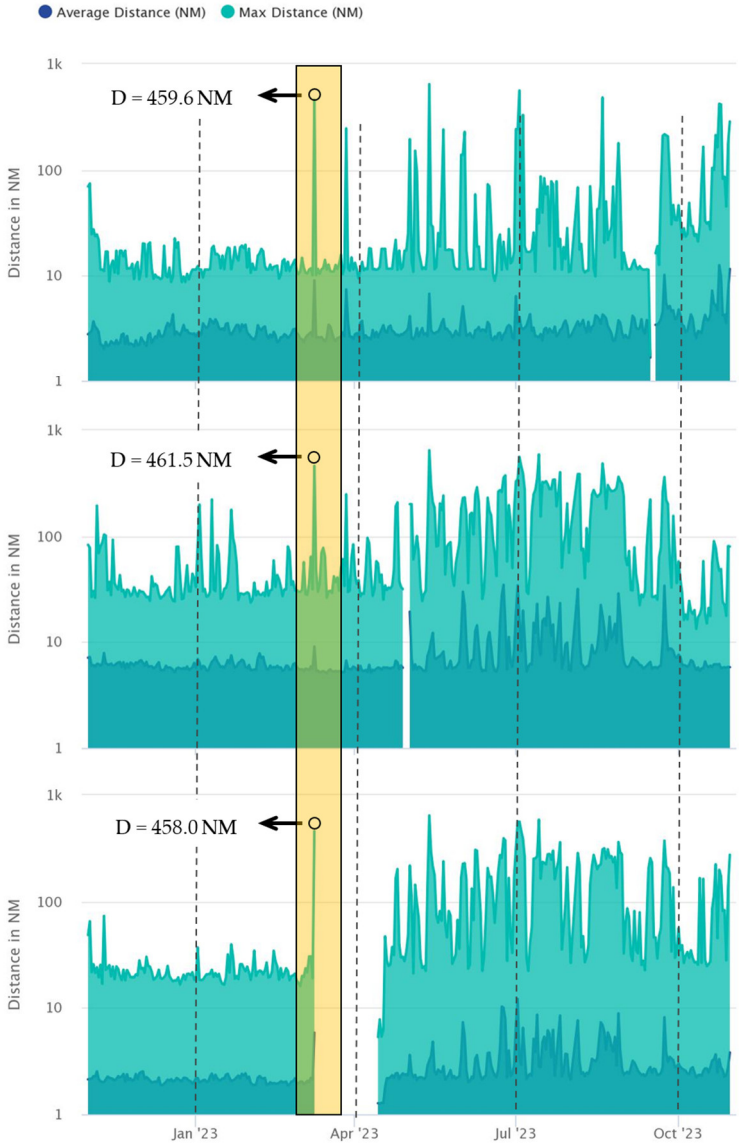


Figure 3. Average and maximum receiving distances of three AIS stations: Costanța Station (h = 41 m), Constanta Kalimbassieris Maritime Station (h = 20 m), Offshore Costanta Station (h = 10 m); source: produced from Marine Traffic.

Table 1. The range of AIS signals in NM.

		Base Station Antenna Height (m)																																		
		4	9	1	25	36	49	64	81	100	121	144	169	196	225	256	289	324	361	400	441	484	529	576	625	676	729	784	841	900	961	1024	1089	1156	1225
Ship station antenna height (m)	4	10.0	12.5	15.0	17.5	20.0	22.5	25.0	27.5	30.0	32.5	35.0	37.5	40.0	42.5	45.0	47.5	50.0	52.5	55.0	57.5	60.0	62.5	65.0	67.5	70.0	72.5	75.0	77.5	80.0	82.5	85.0	87.5	90.0	92.5
	9	12.5	15.0	17.5	20.0	22.5	25.0	27.5	30.0	32.5	35.0	37.5	40.0	42.5	45.0	47.5	50.0	52.5	55.0	57.5	60.0	62.5	65.0	67.5	70.0	72.5	75.0	77.5	80.0	82.5	85.0	87.5	90.0	92.5	95.0
	16	15.0	17.5	20.0	22.5	25.0	27.5	30.0	32.5	35.0	37.5	40.0	42.5	45.0	47.5	50.0	52.5	55.0	57.5	60.0	62.5	65.0	67.5	70.0	72.5	75.0	77.5	80.0	82.5	85.0	87.5	90.0	92.5	95.0	97.5
	25	17.5	20.0	22.5	25.0	27.5	30.0	32.5	35.0	37.5	40.0	42.5	45.0	47.5	50.0	52.5	55.0	57.5	60.0	62.5	65.0	67.5	70.0	72.5	75.0	77.5	80.0	82.5	85.0	87.5	90.0	92.5	95.0	97.5	100.0
	36	20.0	22.5	25.0	27.5	30.0	32.5	35.0	37.5	40.0	42.5	45.0	47.5	50.0	52.5	55.0	57.5	60.0	62.5	65.0	67.5	70.0	72.5	75.0	77.5	80.0	82.5	85.0	87.5	90.0	92.5	95.0	97.5	100.0	102.5
	49	22.5	25.0	27.5	30.0	32.5	35.0	37.5	40.0	42.5	45.0	47.5	50.0	52.5	55.0	57.5	60.0	62.5	65.0	67.5	70.0	72.5	75.0	77.5	80.0	82.5	85.0	87.5	90.0	92.5	95.0	97.5	100.0	102.5	105.0
	64	25.0	27.5	30.0	32.5	35.0	37.5	40.0	42.5	45.0	47.5	50.0	52.5	55.0	57.5	60.0	62.5	65.0	67.5	70.0	72.5	75.0	77.5	80.0	82.5	85.0	87.5	90.0	92.5	95.0	97.5	100.0	102.5	105.0	107.5
	81	27.5	30.0	32.5	35.0	37.5	40.0	42.5	45.0	47.5	50.0	52.5	55.0	57.5	60.0	62.5	65.0	67.5	70.0	72.5	75.0	77.5	80.0	82.5	85.0	87.5	90.0	92.5	95.0	97.5	100.0	102.5	105.0	107.5	110.0

Thus, it can be concluded that a vessel presenting as 450 NM from Costanța is actually quite close to Costanța, since there are no other stations in neighboring Black Sea countries receiving a signal from this vessel, and the other stations are at least 50 NM away from the base stations near Costanța. The method presented for identifying a vessel that is falsifying its position is simple and robust, but a full identification requires an AIS VHF signal information (VSI) string containing the TOA record and RSI information, i.e., the time of arrival and received signal strength.

At present, an AIS is an indispensable system for any vessel traffic service and vessel traffic monitoring center. Each dedicated maritime traffic monitoring application has the ability to set various warning systems, such as automatically displaying all vessels within the traffic zone that are in close proximity to each other or adding an AIS vessel-type filter (80 to 84) to display only tankers, so that only vessels that may be conducting STS operations are displayed. Of course, such a system can also be used to send warnings in the event of near collisions, the loss of an AIS signal, or when a vessel is entering or leaving the traffic zone. Sudden ship movements can be indicated by the ship triggering an alarm at unrealistically high speeds or by a ship coming ashore. Operators or maritime authorities have numerous means at their disposal to ensure the high quality of traffic monitoring, which is essential for safety at sea and the protection of the marine environment.

Various overview charts can be created from the large amount of AIS data, such as displaying major shipping lanes, classifying traffic by vessel type, traffic density, forecasting shipping routes [42], etc. The Figure 4 show the monitoring of shipping routes in the wake of the war between Ukraine and Russia. A quick look at the maritime traffic already shows a change in the shipping routes (marked with yellow dashed circles and ellipse), with tankers from Russia heading toward Costanța (an area off Costanța outside territorial waters) where STS operations are taking place. A very large amount of cargo is also diverted to inland waterways (marked higher on the map).

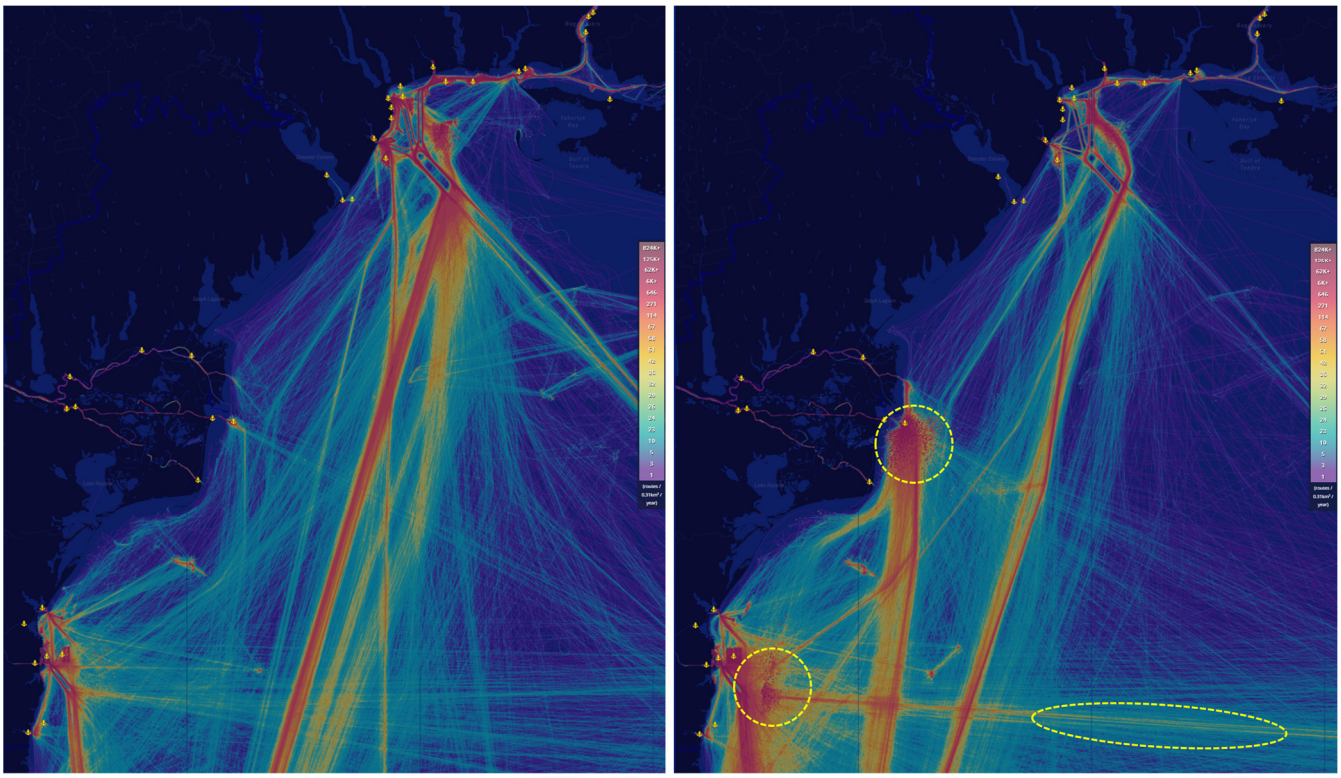


Figure 4. Comparison of traffic density during the years 2021 and 2022; source: produced from Marine Traffic.

Of course, it is also possible to monitor ships outside the radio horizon. The signal from the AIS is broadcast in all directions, including into space, where it is received by AIS onboard satellites, providing a much wider and homogeneous coverage, which is of great value for the overall assessment of maritime traffic. There are three points to note: there is a cost associated with transmitting the data to the shore station; the temporal coverage is much less than a land-based AIS system; and the satellite AIS (S-AIS) does not provide a report from the ship at a specific time interval. Therefore, there is also another complementary, but mandatory, long-range identification and tracking (LRIT) system that requires the ship to send a position report every six hours. Each flag state is required to establish or select an LRIT data center to directly collect LRIT reporting the data from a ship entitled to fly its flag. The LRIT information is always available to the ship's flag state in accordance with the data distribution plan developed by IMO to meet the flag state's requirements. The IMO data distribution plan meets the flag state requirements and is linked to the routing rules. The International LRIT Data Exchange provides the other flag states with valid access to the LRIT data of the ships concerned [43]. LRIT and AISs have many differences, but primarily, AIS is used to avoid collisions, while LRIT is used to monitor specific vessels of interest to the government. These fundamental differences affect both how the self-reporting systems work and how often the self-reports are required. For example, for collision avoidance, only vessels in close proximity need to know a vessel's position; therefore, STS VHF transponders are sufficient. In the case of LRIT, the global nature of the system appears to be the deciding factor in adopting a satellite-based system for transmitting LRIT messages. Unfortunately, we were not able to obtain S-AIS or LRIT data. The latter are of particular interest, as it is currently unknown to what extent LRIT is resistant to spoofing.

2.2. Space-Based Observation and Ship Detection Practices

As for non-cooperative observation systems, the main tools used for maritime surveillance are optical cameras, infrared cameras, and radar. These can be deployed from land, ships, aircrafts, or satellites. Each type of sensor and platform has its strengths and weaknesses in terms of features, such as spatial resolution, update rate, range, coverage, etc. Satellite-based sensors have the particular advantage of remote access, global coverage, regular updates, and comprehensive data collection, making them the only viable option in some scenarios and the most economical in others. The use of satellite imagery is therefore an essential tool for locating ships at sea. In particular, satellite-based radar imagery, usually in the form of synthetic aperture radar (SAR), is very popular for monitoring ships at sea; ships can be detected relatively easily, even through clouds or in the absence of daylight [44,45]. However, interest in the capabilities of optical imaging for maritime surveillance has increased greatly in recent years, perhaps largely due to the growing number of optical imaging satellites. Another technology useful for light detection is the visible infrared imaging radiometer suite (VIIRS) generaly used for detecting ships at night based on light intensity [46]. A detailed literature review of the methods used for detecting and classifying ships using space-based platforms can be found in [47]. There are several satellite platforms for ship detection purposes; but, in this study, we focused on the Sentinel 1 (SAR) and Sentinel 2 (optical) platforms of the European Space Agency's Copernicus program, as they provided accurate quality data and were freely available. To incorporate our scent-based research into further studies, we could also be provided with data from ESA and third-party missions for which we have already applied. This would further improve the ability to accurately represent the ship's position and thus reduce the possibility of the falsification of the presented data on the ship's position. Ship detection with the Sentinel 1 mission (C-band radar) falls into the category of non-cooperative systems and enables the detection of ships that do not have AISs or other vessel monitoring systems on board, e.g., the VMS of fishing vessels. With two platforms (Sentinels 1A and 1B), the system has a revisit time of only a few days, which is a great opportunity for ship detection. The most suitable mode for ship detection is the interferometric wide angle (IW), which covers an

extended area with a width of 250 km at a spatial resolution of 20 × 22 m and ensures the detection of larger ships, such as shuttle tankers, in almost all weather conditions. The most suitable polarization for object detection at sea is VH (Vertical transmit-horizontal receive). The Sentinel application platform (SNAP) was used to analyze the SAR images in this study. SNAP is a pixel-based algorithm that uses a systematic method to identify and eliminate false alarms from objects on the sea surface. The constant false alarm rate (CFAR) method was used to determine the threshold for an object to be indicated as a vessel at sea.

The Sentinel 1-SAR workflow for ship detection consists of three steps: pre-processing (removing thermal noise, loading a new orbit file, performing the ternary correction, creating a subset, and masking the land area), object detection with the built-in CFAR algorithm, and finally extracting the ships' positions.

The Copernicus Sentinel-2 missions of 2 identical satellites provide free multispectral images with a maximum update rate of 5 days and a resolution of up to 10 m (4 bands out of 13). Both satellites, Sentinels 2A and 2B, are in the same orbit at a mean altitude of 786 km and are separated by 180 degrees, which is the basis for the systematic coverage of all continental land areas (including inland waters) between 56° South and 82.8° North latitudes. More importantly, for ship tracking, it also covers all coastal waters up to 20 km from the coast, all islands with an area larger than 100 km^2, all EU islands, all enclosed seas, and the entire Mediterranean. With an orbital swath of 290 km, optical images can not only be used for ship detection purposes, but also for identification, i.e., target classification, which is quite a challenging task and is well described in [48]. A multispectral approach based on optical learning can be used both on the high seas and in harbors and eliminates the need to store a vector map of coastlines.

3. Results of the Case Studies

Since the beginning of the war in Ukraine began, Russian ships have been banned from docking in European Union ports; however, Russian oil and oil derivatives have managed to circumvent the sanctions and reach Europe. The maritime world is probably facing an unprecedented period of fraudulent shipping practices by tanker operators trying to circumvent the sanctions. Inspired and encouraged by the research of Bergman [49], Windward [50], and Savchuk [51], we systematically investigated how Russian oil has circumvented EU sanctions to reach European ports.

European Union sanctions prohibit Russian ships from docking in EU ports. Nevertheless, new shipping activities were observed off the Romanian coast in the spring of 2022. The 20-year-old Liberian-flagged crude oil tanker New Legend anchored off the coast of Constanța on 24 April 2022. The ship did not move for several months and served as a storage tanker for the transshipment of oil of Russian origin; other tankers soon appeared on the scene. Figure 5 shows the spatial distributions of vessel traffic in 2021 (left) and 2022 (right), with the location of the transshipment clearly visible.

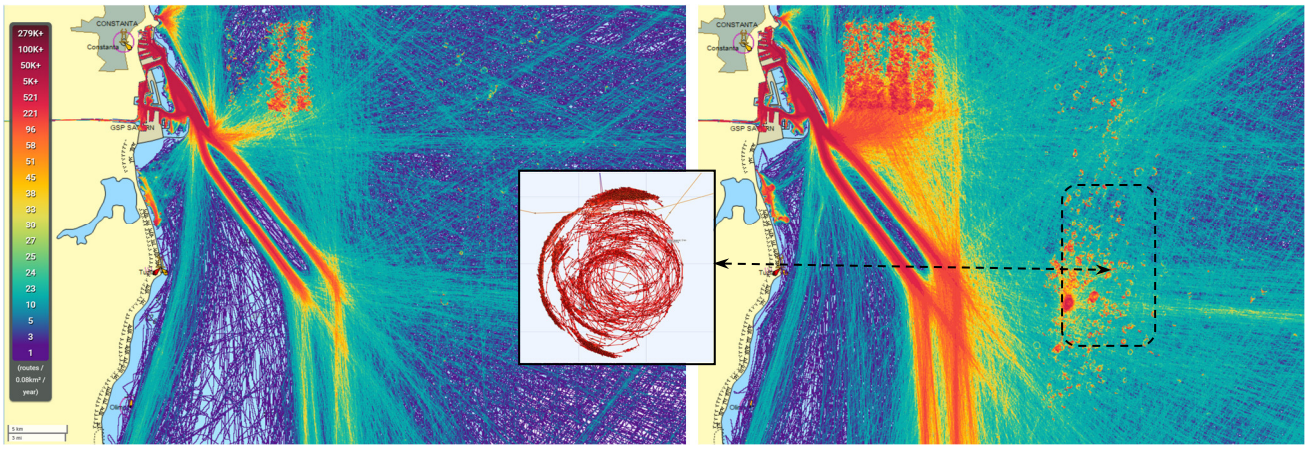


Figure 5. AIS traces of STS operations near the port of Costanţa; source: produced from Marine Traffic.

The middle part of Figure 5 shows the track of the New England, which lay at anchor for several months, during which time it received cargo from a number of smaller Russian tankers. The transshipment activity in the first two weeks is shown in the Table 2. Laden Russian tankers called at New England and then sailed back to the area of Novorossiysk or though the Azov Sea up to the port of Svetlyy Yar on the Volga River. With a carrying capacity of almost 160,000 tons, New England can store cargo of more than 20 VF-class tankers. After ten tankers had discharged their cargo to the storage tanker, two tankers, Beks Swan and Kimolos Warrior, took on the cargo, the latter discharging onto Nordic Cosmos in the Laconian Gulf on 20 May 2022. Beks Swan did not sail into the Black Sea last year, but regularly took on cargo in three Russian Baltic ports. At this point, it should be noted that, both in the areas off Costanța and in the Laconian Gulf, where STS operations were conducted even closer to the coast, the tankers were also assisted by local tugboats when approaching the storage tankers, suggesting that the authorities were aware of all the activities taking place. On May 5, an additional transshipment also occurred on the coast off Costanța, with the storage tanker Haifa Adumello taking on the cargo of the tanker VF-8.

Table 2. First transshipment operations off the coast of Costanța.

Date	Offloading Vessel	Loading Vessel	AIS	Satellite
24 April 2022	VF-4		On	
25 April 2022	VF-5		On	
28 April 2022	VF-21		On	
1 May 2022	VF-18		On	
1 May 2022	VF-13		On	
1 May 2022	VF-6		Off	
2 May 2022	VF-12		On	
3 May 2022	VF-4		On	
3 May 2022	Kapitan Permyakov		On	
5 May 2022	VF-21		On	
6 May 2022		Beks Swan	Off	
7 May 2022	VF-5	Beks Swan	Off	Sentinel-2
7 May 2022		Kimolos Warrior	Off	

Two interesting cases are those of Beks Swan and the tanker VF-5, which were simultaneously involved in a cargo transfer, where both switched off their AISs, the larger tanker for 24 h. Figure 6 (Sentinel-2 L2A true-color image from 7 May 2022) shows in yellow dashed circles both tankers moored to New Legend.

To confirm the deliberate deactivation of the vessel's AIS system, the reception of the AIS base stations must first be checked. However, it could be assumed that there was a deliberate deactivation, as in this case, all other vessels in the vicinity of New England were seen by the AIS signals. To confirm the AIS coverage of the STS site, we provided the AIS reception statistics for the Mediterranean and Black Sea compiled by the European Maritime Safety Agency (EMSA), where the Mediterranean AIS Regional Exchange System (MAREΣ) was available [52]. The estimated monthly AIS coverage of the MAREΣ is represented by layers, as shown in Figure 7.

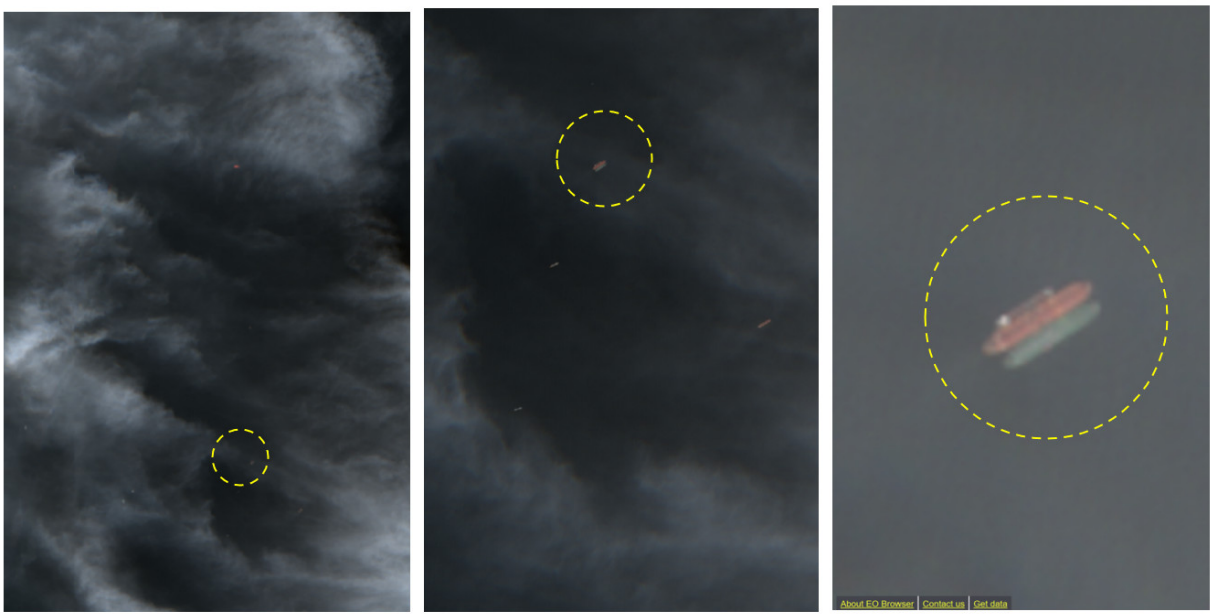


Figure 6. Satellite optical image, Sentinel-2 (7 May 2022, 09:08:20). The large ship in the middle is the storage tanker New England, on the port side is the Russian tanker VF-5, and on the starboard side is the tanker Beks Swan flying the flag of the Marshall Islands.

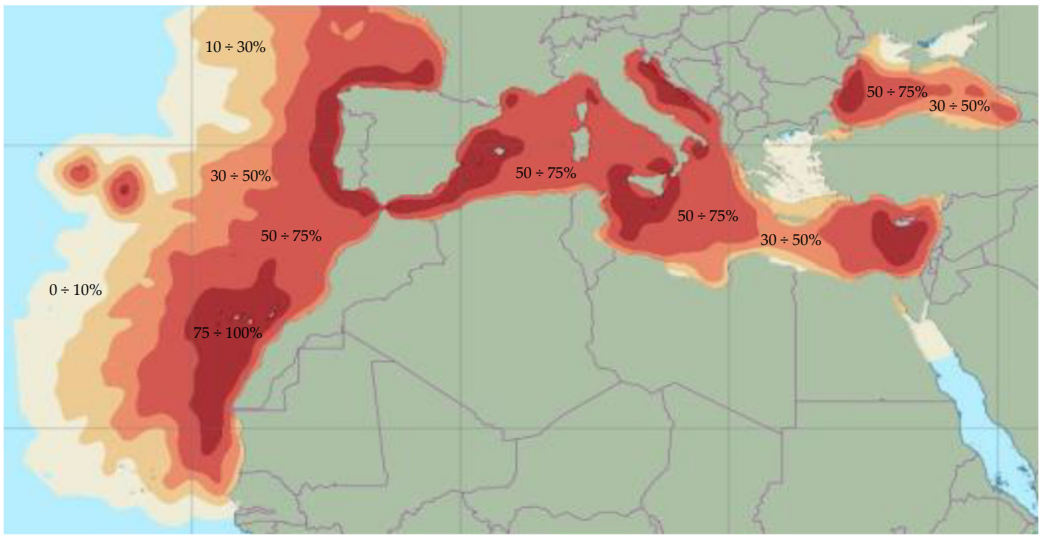


Figure 7. The estimated monthly AIS coverage of the MAREΣ 2022 [52].

Each layer was assigned to an area and corresponded to a probability range for the reception of AIS information from the vessels. The following probability ranges were evident: 0–10%, 10–30%, 30–50%, 50–75%, and 75–100%. The area in which STS operations were conducted off the coast of Constanța was well covered, with a detection probability between 75 and 100%.

Figure 8 shows the turnover of all VF tankers and some transshipment tankers deployed from May to September 2023. It can be seen that Russian oil traffic is also routed to ports within the EU.

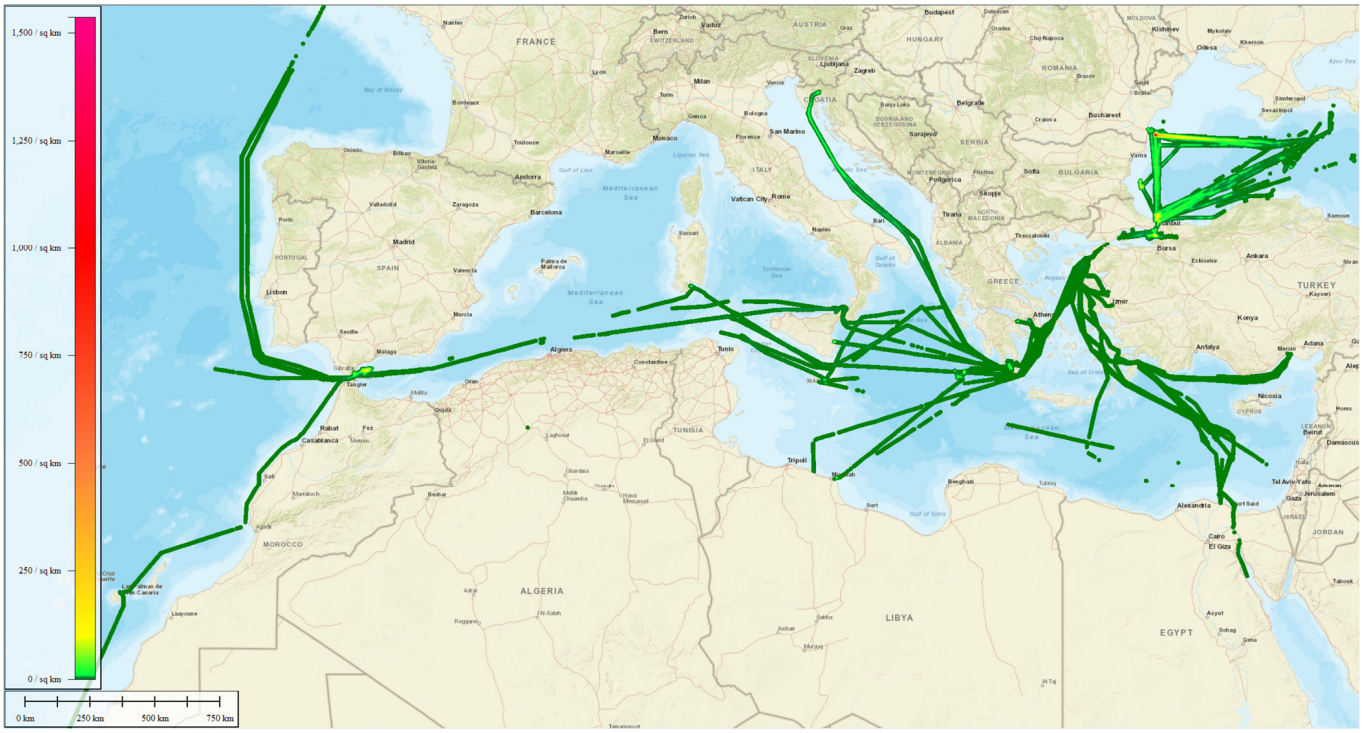
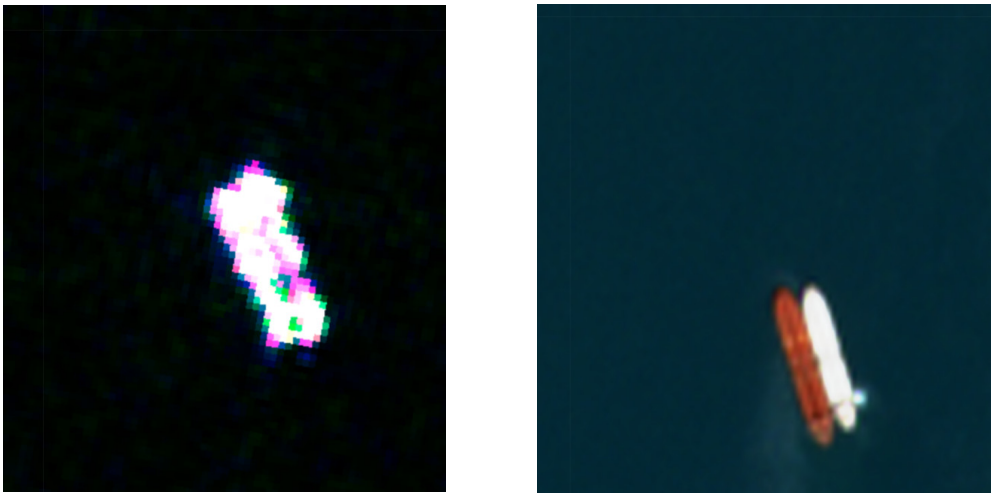


Figure 8. The Black Sea oil STS transfer activities and its transit from May to September 2022.

During the investigation, we were also able to follow the transshipment from start to finish. On 2 July 2022, New Legend transferred its cargo to the tanker San Sebastian in 434 min (Figure 9). The STS operations were monitored by the two satellite platforms SAR and Optical.



(**a**) (**b**)

Figure 9. Tankers New Legend and San Sebastian on 2 July 2022: (**a**) radar image as it appears on Sentinel-1; (**b**) optical image as it appears on Sentinel-2.

The complexity of tracking tankers involved in the Russian oil business is illustrated in Figure 10, which shows the route of the tanker Kriti Future over several months, calling at Russian ports, the STS site in Greece, and several other ports, many of which are in EU countries.

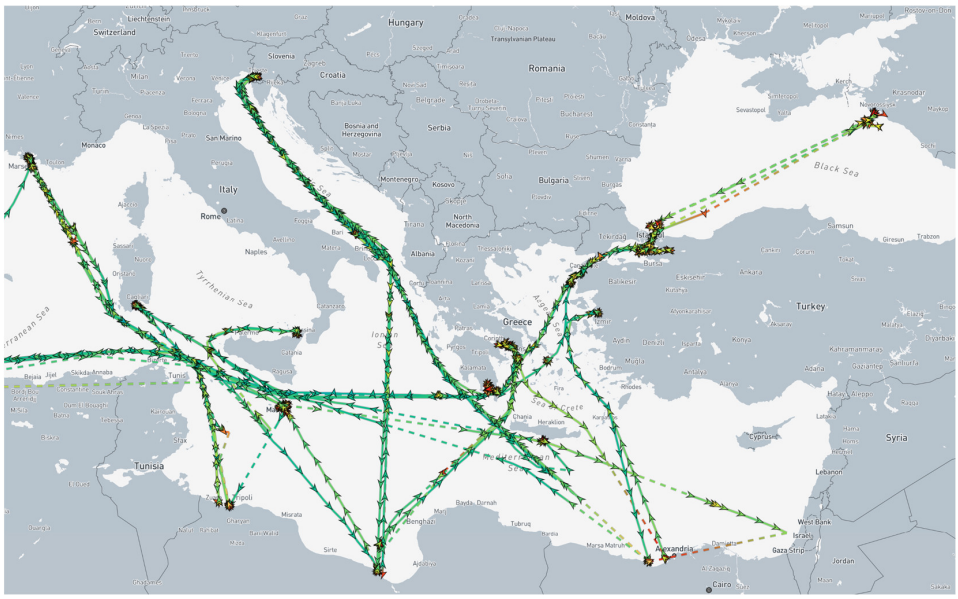


Figure 10. Trajectory of Kriti Future tanker; source: adapted from Marine Traffic.

Like Bergman [49], we found that Russian-flagged tankers often switched off their transponders, making it difficult to track their movements. The misuse of AIS collision avoidance signals jeopardizes maritime safety by increasing the risk of collisions, oil spills, and other serious accidents. A combination of satellite imagery and AIS data from the tankers shows that, while the tankers reported their position in the western Black Sea, sometimes for weeks, their true position was near the Kerch Strait, 400 miles to the northeast. Many of these tankers are substandard and do not comply with international maritime safety regulations. This significantly increases the risk of dangerous accidents and oil spills, with disastrous consequences for seafarers, coastal states, and the marine environment.

The example in Figure 11 shows another STS operation with Russian oil. However, here, the tanker did not want to reveal its actual position, so this ship did not switch off the AIS system and became a so-called "dark tanker". It falsified its position and displayed it in a different location than where it actually was, performing a spoofing activity that could be very dangerous. We became aware of this vessel because, according to the AIS system, it almost collided with another vessel in the STS area (Laconian Bay), which also reduced its speed, as such a vessel appeared on the electronic chart display and information system (ECDIS) and radio detection and ranging (RADAR) screens, but not on the actual horizon. The tanker Turba had intercepted Strea as she was heading into the sunset and must have been surprised by the alerts from her navigation system. Turba's rapid course change was also very unusual, apparently performing an impossible maneuver.

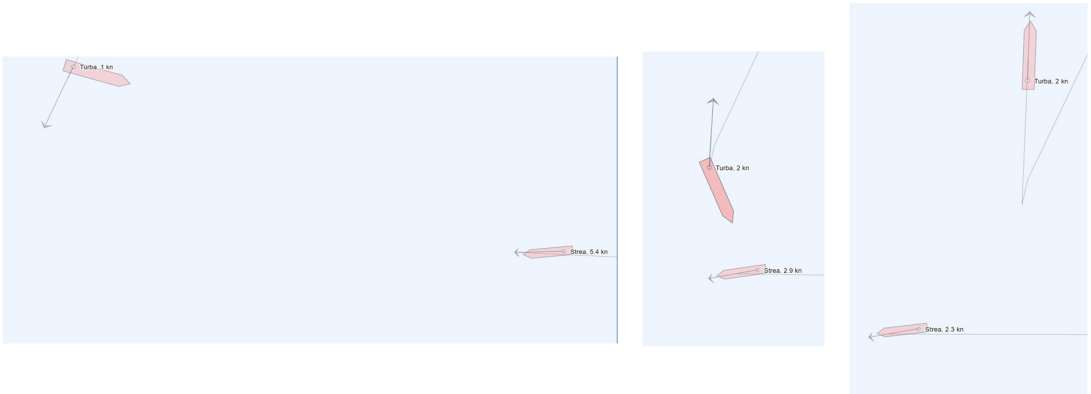


Figure 11. A look-a-like near miss with a false AIS position.

Sentinel-1 images were available and captured the situation just minutes before the apparent near miss. Using SNAP application, we processed the image and exported the detected vessels to the GIS application, into which we also imported the AIS data. It immediately became clear that there was no Turba tanker in the vicinity of the Strea vessel, which was actually performing an STS operation with the Simba tanker, i.e., Turba was showing an incorrect position; at this time, the offset was 6 NM, as shown in Figure 12. Furthermore, the movement and orientation of the vessel did not match the movement of the Simba tanker. We also checked the optical images, and the following day, 20 September 2023, we observed the same situation: Turba was still falsifying its AIS transmission. Such activities are very dangerous and the maritime authority should significantly increase its vigilance and sanction such culprits.

Figure 12. SAR image from 19 September 2023 and optical image from 20 September 2023 showing the AIS spoofing of the tanker Turba during an STS operation in a busy area. The SAR image as well as the optical image shows that the Turba tanker is located next to the Simba tanker while the AIS image shows a large offset.

Previously, on 14 September 2023, the tanker Simba had taken on cargo at the familiar offshore location of Costanța from the tanker New Trust, which had taken on cargo from the tanker VF-4 at the same time. Simba had communicated with New Trust with the help of the two tugs Vulkan and Dynamax. It should be emphasized once again that these operations occurred off the coast of Costanța, albeit outside territorial waters, but with the help of port resources. The situation is similar off the coast of Malta. In the Gulf of Laconia, STS operations are conducted in the immediate vicinity of the coast. The main point in this regard is that such dangerous and illegal activities are more common than we can express at this point.

4. Discussion

The international community is making great efforts to curb the trade in Russian crude oil. Last December, the Price Cap Coalition (EU, G7, and Australia) responded to the ongoing Russian invasion of Ukraine by capping the price of Russian seaborne oil sold to global markets. Companies based in the coalition countries are currently allowed to provide services that support the sale of Russian oil, including shipping, insurance, and trade finance, but only if the price paid to Russia does not exceed USD 60 per barrel. The goal of the coalition is to reduce Russian revenues received from oil sales while ensuring the uninterrupted flow of Russian oil to global markets, thus preventing a negative supply shock that can have short-term negative consequences for the rest of the world [53]. However, a report by the Centre for Research on Energy and Clean Air (CREA) shows that, following Moscow's invasion of Ukraine, some countries have increased their imports of Russian oil and have processed ("laundered") it into products that are sold to countries that have imposed sanctions on Russian oil, the so-called "laundromat" countries [54]. Our research confirms that Russian oil is finding its way to countries at limited prices in the form of diesel, jet fuel, and petrol.

The data from CREA [54] are remarkable: in the 12 months following the invasion of Ukraine, the EU spent USD 19.3 billion on these Russian-origin products, followed by Australia with USD 8.74 billion, the United States with USD 7.21 billion, the United Kingdom with USD 5.46 billion, and Japan with USD 5 billion.

It goes without saying that the armed conflict in Ukraine has triggered a multitude of sanctions affecting the industry. In addition to the suspicion of STS oil transfers mentioned in the article, there is also a new type of fraud that has been introduced to the global community: vessel identity laundering (VIL). According to Tsakiris [55], this is a novel tactic whereby one or more vessels assume a different identity on an AIS in order to provide "dirty" vessels (i.e., those associated with illegal activities) with a "clean" identity, and where at least one vessel in this operation assumes an identity obtained through IMO number fraud (Unmasked-vessel identity laundering). With the sale of older tankers increasing, there is a possibility that this can soon increase. One hopes that serious ship owners want to avoid being involved in illegal transactions. From the points of view of security and environmental risks, the emergence of these shadow ships and the countries willing to host them is worrying for all those involved in the maritime industry. There is little to discourage their activities. Yet, the shadow fleet is almost entirely composed of ships that are past their prime and on their way to the scrapyard, and this is a growing and increasingly dangerous set of circumstances. These vessels sail under flags of convenience, which are subject to less stringent legislations and allow for lower maintenance standards. This has led to the fleets and ships engaged in legal traffic being exposed to a greater risk of accidents. Accidents involving shadow tankers have increased worldwide, such as fires, groundings, and pollution. In 2022, there were eight groundings, collisions, or near misses involving tankers carrying sanctioned crude oil or oil products [1]. One example from 2023 is the m/v Pablo, which was part of the world's growing fleet of shadow tankers that caught fire, exploded, and completely burnt down off the coast of Malaysia, not far from the busy Singapore Strait. Fortunately, the tanker was not loaded with oil, so the environmental damage caused was limited [2] and therefore did not attract public

attention. If the ship had been carrying oil, there would have been an environmental disaster with about 600,000 barrels being spilled. To this day, the wreckage of the ship remains untouched where the accident occurred because no one is willing to send out a salvage crew and because no one knows who will pay for it. So, the case remains unsolved and is a typical example of what happens when there is an environmental disaster [56].

The analysis shows that the falsification of the AIS led to a tripling in the size of the so-called dark fleet that transported illegal oil from Russia around the world. By tracking ships during this study, it was discovered that many shadow tankers changed their names and registries, some virtually after every voyage, their ownership remaining a mystery.

The data provided by Geollect [57] show that, since 14 May 2023, the data from commercial vessels' AISs are remotely spoofed to create the impression of a 65 km Z symbol on the Black Sea, as seen on the open source tracking software (Figure 13). The tracks that created the image indicate high ship speeds of 102 knots (188 km per hour), which is another indication that it is fake. The perpetrator behind the spoofing may have used high-frequency signals to mimic a real signal with ease, causing the ship's signal to display false information.

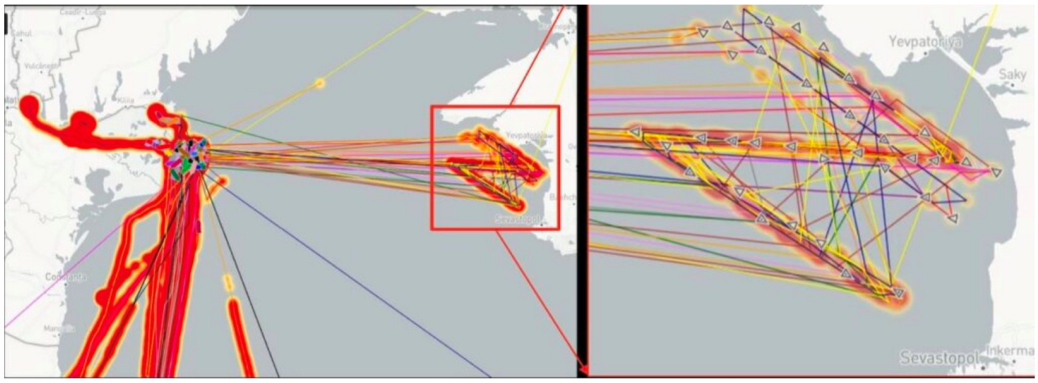


Figure 13. AIS spoofing data projecting a Z symbol on the Black Sea during 14–21 May 2023; source: Geollect [57].

5. Conclusions

Geopolitics and the maritime ecosystem are interdependent and complicated, and maritime risks are constantly evolving. This article shows how much things have changed in unpredictable ways over just the last 18 months. This research was conducted using predictive analytics and an artificial intelligence platform. Without these tools, it would be almost impossible to keep up with the maritime risks occurring at present due to the flood of data and their complexity. But, to also improve the quality of the input data, it will be necessary in future studies to plan, combine, and compare the data from several different platforms, e.g., the ESA oil-trading analytics monitor (OTAM) and ship detection systems, to determine the ship's position more accurately.

With the looming global recession and economic sanctions from the West, combined with the political and security situations in the neighboring eastern countries, we can expect to see an increase in fraudulent maritime practices, particularly a combination of illegal activities, GNSS manipulation, and secret STS meetings. Most likely, new nodes will continue to emerge to disguise illegal activities, while the old ones will be less effective.

The false-position data sent by the tanker Beks Swan demonstrates the importance of developing robust automated systems to detect and flag the fraudulent use of AISs. Otherwise, it will not be long before we can no longer trust AISs. The international community has taken decisive action to restrict the sale of Russian crude oil to fund the armed conflict, but these measures will be ineffective if AIS falsifications go undetected. This article showed that false positions could be detected with the data methods currently available. We can be confident that the increasing automation of these methods will soon mean that any ship falsifying its position will only end up attracting attention to its illegal

activities, which are also linked to the complex and multi-layered shadow fleet. The impact of Russian sanctions has meant that the number of these vessels has doubled in the last 18 months. This is a worrying development that threatens the world fleet and the environment. With collaborative action and cooperation from all stakeholders, substandard ships can be prevented from threatening our maritime industry and our environment. Yet, to date, no action has been taken. Legislations need to be strengthened so that the standards of the individual countries that issue ships with certificates for the transport of dangerous goods (oil) are complied with. The fundamental problem is that, where profits are involved, political will tends to be compromised.

It is very difficult to understand that, on the one hand, we are still encountering ships in the maritime world that should have been consigned to the scrapyard long ago, while on the other hand, the maritime industry is making every effort to address the increasing cyber risks by building cyber security systems into ship designs that enables strong protection against threats while ensuring compliance with the new regulations of the International Association of Classification Societies (IACS) Unified Requirements (URs) E27 and E26 [58], which complement the IMO cyber security regulations that have been in force since 1 January 2021.

In our view, the deployment of multiple public and private satellite navigation constellations that do not rely on signal transmissions should provide the shipping industry with much-needed improved protection against criminal activity at sea in the foreseeable future.

Author Contributions: Conceptualization, A.A., I.P. and M.P.; methodology, M.P.; software, M.P. and L.G.; validation, A.A., M.P., I.P. and L.G.; formal analysis, P.V. and L.G.; investigation, A.A., I.P. and M.P.; resources, A.A. and M.P.; data curation, P.V.; writing—original draft preparation, A.A., I.P., P.V. and M.P.; writing—review and editing, A.A., L.G. and M.P.; visualization, A.A.; supervision, M.P. and L.G.; project administration, P.V.; funding acquisition, P.V. All authors have read and agreed to the published version of the manuscript.

Funding: This research received no external funding.

Institutional Review Board Statement: Not applicable.

Informed Consent Statement: Not applicable.

Data Availability Statement: The data for this analysis were obtained from the Maritime Administration Office in Slovenia and the ELMAN S.r.l in Italy.

Acknowledgments: We thank Elman S.r.l for their assistance with the analysis of the AIS data, UL FPP postgraduate student Migel Mehlmauer and US proofreader Rick Harsch.

Conflicts of Interest: The authors declare no conflict of interest.

Abbreviations

AIS	Automated Identification System
BIMCO	Baltic and International Maritime Council
CFAR	Constant False Alarm Rate
CREA	Centre for Research on Energy and Clean Air
ECDIS	Electronic Chart Display and Information System
EEZ	Exclusive Economic Zone
EMSA	European Maritime Safety Agency
EU	European Union
ESA	European Space Agency
FIS	Fuzzy Interference System
GIS	Geographic Information System
GNSS	Global Navigation Satellite System
GPS	Global Positioning System
HAZOP	Hazard and Operability Process Analysis
IACS	International Association of Classification Societies
IMO	International Maritime Organization

IW	Interferometric Wide
LNG	Liquefied Natural Gas
LRIT	Long-Range Identification and Tracking
MAREΣ	Mediterranean AIS Regional Exchange System
MARPOL	International Convention for the Prevention of Pollution from Ships
MMSI	Maritime Mobile Service Identity
MSA	Maritime Situational Awareness
NM	Nautical Mile
OTAM	Oil-Trading Analytics Monitor
PFMEA	Process Failure Mode and Effect Analysis
RADAR	Radio Detection and Ranging
ROT	Rate Of Turn
RSI	Received Signal Strength
SAR	Synthetic Aperture Radar
S-AIS	Satellite AIS
SNAP	Sentinel Application Platform
SOLAS	International Convention for the Safety of Life at Sea
STPA	System Theoretical Process Analysis
STS	Ship To Ship
TOA	Time Of Arrival
TTWs	Territorial Waters
URs	Unified Requirements
VH	Vertical Transmit–Horizontal Receive
VHF	Very High Frequency
VIIRS	Visible Infrared Radiometer Suite
VIL	Vessel Identity Laundering
VMS	Vessel Monitoring System
VSI	VHF Signal Information

References

1. Insight: Oil Spills and Near Misses: More Ghost Tankers Ship Sanctioned Fuel. Available online: https://www.reuters.com/business/autos-transportation/oil-spills-near-misses-more-ghost-tankers-ship-sanctioned-fuel-2023-03-23/ (accessed on 23 September 2023).
2. The Diplomat: Southeast Asian States Need to Tackle the Dangerous Shadow Tanker Activities in Their Waters. Available online: https://thediplomat.com/2023/09/ (accessed on 23 September 2023).
3. ICS/OCIMF. *Ship to Ship Transfer Guide (Petroleum)*, 4th ed.; Witherby Publishing Group: Livingston, UK, 2005.
4. Ventikos, N.P.; Stavrou, D.I. Ship to Ship (STS) Transfer of Cargo: Latest Developments and Operational Risk Assessment. *SPOUDAI J. Econ. Bus.* **2013**, *63*, 172–180.
5. Tokić, T.; Frančić, V.; Hasanspahić, N.; Rudan, I. Training Requirements for LNG Ship-to-Ship Transfer. *Pomor. Zbornik.* **2021**, *60*, 49–63. [CrossRef]
6. CDI/ICS/OCIMF/SIGTTO. *Ship to Ship Transfer Guide for Petroleum, Chemicals and Liquefied Gases*, 1st ed.; Witherby Seamanship: Livingston, UK, 2013; pp. 13–15. ISBN 9781856095945.
7. Shipowners Security for Small and Specialist Vessels, Buletin, Issue Date 27/01/2015, Ship to Ship Oil Transfer Operations: We Would Like to Advise Members of Claims Arising from Poor Cargo Practices Being Adopted on Board Tankers. Available online: https://www.shipownersclub.com/media/2015/01/Ship-to-Ship-oil-transfer-operations.pdf (accessed on 17 April 2023).
8. IMO Resolution MEPC.186(59). *Amendments to the Annex of the Protocol of 1978 Relating to the International Convention for the Prevention of Pollution from Ships, 1973*; IMO Publishing: London, UK, 2009.
9. Stavrou, D.I.; Ventikos, N.P. Ship to Ship Transfer of Cargo Operations: Risk Assessment Applying a Fuzzy Inference System. *J. Risk Anal. Crisis Response* **2014**, *4*, 214–227. [CrossRef]
10. Stavrou, D.I.; Ventikos, N.P. Risk evaluation of Ship-to-Ship transfer of cargo operations by applying PFMEA and FIS. In Proceedings of the 2015 Annual Reliability and Maintainability Symposium (RAMS), Palm Harbor, FL, USA, 26–29 January 2015; pp. 1–7. [CrossRef]
11. Sultana, S.; Okoh, P.; Haugen, S.; Vinnem, J.E. Hazard analysis: Application of STPA to ship-to-ship transfer of LNG. *J. Loss Prev. Process Ind.* **2019**, *60*, 241–252. [CrossRef]
12. Suspicion of Illegal Ship-to-Ship Transfers of Goods by North Korea-Related Vessels. Available online: https://www.mofa.go.jp/fp/nsp/page4e_000757.html (accessed on 22 April 2023).
13. Sanctions and STS Transfers—Legal Risks. Available online: https://www.skuld.com/topics/legal/sanctions/sanctions-and-sts-transfers--legal-risks/ (accessed on 22 April 2023).

14. United Nations Security Council. S/2021/777. Letter Dated 3 September 2021 from the Panel of Experts Established Pursuant to Resolution 1874 (2009) Addressed to the President of the Security Council. Available online: https://www.securitycouncilreport.org/atf/cf/%7B65BFCF9B-6D27-4E9C-8CD3-CF6E4FF96FF9%7D/S_2021_777_E.pdf (accessed on 22 April 2023).
15. UKPANDI. Circular 01/22 Sanctions—Recent Deceptive Practices. Available online: https://www.ukpandi.com/news-and-resources/circulars/2022/circular-0122-sanctions-recent-deceptive-practices/ (accessed on 22 April 2023).
16. ReCAAP ISC. *Regional Guide to Counter Piracy and Armed Robbery against Ships in Asia*; ReCAAP ISC: Singapore, 2016; p. 5. Available online: https://www.american-club.com/files/files/Regional_Guide_to_Counter_Piracy_and_Armed_Robbery_Against_Ships_in_Asia.pdf (accessed on 22 April 2023).
17. Kamal-Deen, A. The Anatomy of Gulf of Guinea Piracy. *Nav. War Coll. Rev.* **2015**, *68*, 93–118. Available online: https://digital-commons.usnwc.edu/nwc-review/vol68/iss1/7/ (accessed on 22 April 2023).
18. Windward. High Sea Russian Oil Transfers Are Far from the Only Smuggling Method. Available online: https://windward.ai/blog/high-sea-russian-oil-transfers-are-far-from-the-only-smuggling-method/ (accessed on 18 April 2023).
19. Goudossis, A.; Katsikas, S.K. Towards a secure automatic identification system (AIS). *J. Mar. Sci. Technol.* **2019**, *24*, 410–423. [CrossRef]
20. Ramin, A.; Masnawi, A.; Shaharudin, A. Prediction of Marine Traffic Density Using Different Time Series Model from AIS Dana of Port Klang and Straits of Malacca. *Trans. Marit. Sci.* **2020**, *2*, 217–223. [CrossRef]
21. Eriksen, T.; Greidanus, H.; Delaney, C. Metrics and provider-based results for completeness and temporal resolution of satellite-based AIS services. *Mar. Policy* **2018**, *93*, 80–92. [CrossRef]
22. Natale, F.; Gibin, M.; Alessandrini, A.; Vespe, M.; Paulrud, A. Mapping fishing effort through AIS data. *PLoS ONE* **2015**, *10*, e0130746. [CrossRef]
23. Pallotta, G.; Vespe, M.; Bryan, K. Vessel Pattern Knowledge Discovery from AIS Data: A Framework for Anomaly Detection and Route Prediction. *Entropy* **2013**, *15*, 2218–2245. [CrossRef]
24. Perkovic, M.; Twrdy, E.; Harsch, R.; Vidmar, P.; Gucma, M. Technological Advances and Efforts to Reduce Piracy. *TransNav* **2012**, *6*, 203–206.
25. Lee, E.S.; Mokashi, A.J.; Moon, S.J.; Kim, G.S. The Maturity of Automatic Identification Systems (AIS) and Its Implications for Innovation. *J. Mar. Sci. Eng.* **2019**, *7*, 287. [CrossRef]
26. Fournier, M.; Hilliard, R.C.; Rezaee, S.; Pelot, R. Past, present, and future of the satellite-based automatic identification system: Areas of applications (2004–2016). *WMU J. Marit. Aff.* **2018**, *17*, 311–345. [CrossRef]
27. Soldi, G.; Gaglione, D.; Ramponi, S.; Forti, N.; D'Afflisio, E.; Kowalski, P. Monitoring of Critical Undersea Infrastructures: The Nord Stream and Other Recent Case Studies. *IEEE Aerosp. Electron. Syst. Mag.* **2023**, *38*, 4–24. [CrossRef]
28. IALA Guideline G1082. An Overview of AIS, Edition 2.1. IALA-AISM. 2016. Available online: https://www.iala-aism.org/product/g1082/ (accessed on 20 April 2023).
29. Kessler, G.C. Protected AIS: A Demonstration of Capability Scheme to Provide Authentication and Message Integrity. *TransNav* **2020**, *14*, 279–286. [CrossRef]
30. Caprolu, M.; Di Pietro, R.; Raponi, S.; Sciancalepore, S.; Tedeschi, P. Vessels Cybersecurity: Issues, Challenges, and the Road Ahead. *IEEE Commun. Mag.* **2020**, *58*, 90–96. [CrossRef]
31. Balduzzi, M.; Wilhoit, K.; Pasta, A. A Security Evaluation of AIS. *Trend Micro Res. Pap.* **2018**, 1–9. [CrossRef]
32. Iphar, C.; Napoli, A.; Ray, C. An expert-based method for the risk assessment of anomalous maritime transportation data. *Appl. Ocean Res.* **2020**, *104*, 102337. [CrossRef]
33. Iphar, C.; Ray, C.; Napoli, A. Uses and Misuses of the Automatic Identification System. In Proceedings of the IEEE OCEANS 2019, Marseille, France, 17–20 June 2019. [CrossRef]
34. Salmon, L.; Ray, C.; Claramunt, C. Continuous detection of black holes for moving objects at sea. In Proceedings of the 7th ACM SIGSPATIAL International Workshop on GeoStreaming, Burlingame, CA, USA, 31 October–3 November 2016. IWGS '16. [CrossRef]
35. IMO. *The International Convention for Safety of Life at Sea (Consolidated Edition 2020)*; IMO Publishing: London, UK, 2020; pp. 15, 34. ISBN 9789280116908.
36. IMO Resolution A.1106(29). *Revised Guidelines for the Onboard Operational Use of Shipborne Automatic Identification Systems (AIS)*; IMO Publishing: London, UK, 2015.
37. BIMCO. AIS Switch Off Clause 2021. Available online: https://www.bimco.org/contracts-and-clauses/bimco-clauses/current/ais_switch_off_clause_2021 (accessed on 22 April 2023).
38. Androjna, A.; Brcko, T.; Pavic, I.; Greidanus, H. Assessing Cyber Challenges of Maritime Navigation. *J. Mar. Sci. Eng.* **2020**, *8*, 776. [CrossRef]
39. Androjna, A.; Perkovič, M.; Pavic, I.; Mišković, J. AIS Data Vulnerability Indicated by a Spoofing Case-Study. *Appl. Sci.* **2021**, *11*, 5015. [CrossRef]
40. Han, J.; Wu, J.; Zhang, L.; Wang, H.; Zhu, Q.; Zhang, C.; Zhao, H.; Zhang, S. A Classifying-Inversion Method of Offshore Atmospheric Duct Parameters Using AIS Data Based on Artificial Intelligence. *Remote Sens.* **2022**, *14*, 3197. [CrossRef]
41. Tang, W.; Cha, H.; Wei, M.; Tian, B. The effect of atmospheric ducts on the propagation of AIS signals. *Aust. J. Electr. Electron. Eng.* **2019**, *16*, 111–116. [CrossRef]

42. Sigillo, L.; Marzilli, A.; Moretti, D.; Grassucci, E.; Greco, C.; Comminiello, D. Sailing the Seaformer: A Transformer-Based Model for Vessel Route Forecasting. In Proceedings of the 2023 IEEE 33rd International Workshop on Machine Learning for Signal Processing (MLSP), Rome, Italy, 17–20 September 2023; pp. 1–6. [CrossRef]
43. Cheng, Y. Satellite-based AIS and its Comparison with LRIT. *TransNav* **2014**, *8*, 183–187. [CrossRef]
44. Zhang, T.; Zeng, T.; Zhang, X. Synthetic Aperture Radar (SAR) Meets Deep Learning. *Remote Sens.* **2023**, *15*, 303. [CrossRef]
45. Passah, A.; Sur, S.N.; Abraham, A.; Kandar, D. Synthetic Aperture Radar image analysis based on deep learning: A review of a decade of research. *Eng. Appl. Artif. Intell.* **2023**, *1*, 123. [CrossRef]
46. Marzuki, M.I.; Rahmania, R.; Kusumaningrum, P.D.; Akhwady, R.; Sianturi, D.S.; Firdaus, Y.; Sufyan, A.; Hatori, C.A.; Chandra, H. Fishing boat detection using Sentinel-1 validated with VIIRS Data. *IOP Conf. Ser. Earth Environ. Sci.* **2021**, *925*, 012058. [CrossRef]
47. Kanjir, U.; Greidanus, H.; Oštir, K. Vessel detection and classification from spaceborne optical images: A literature survey. *Remote Sens. Environ.* **2018**, *207*, 1–26. [CrossRef]
48. Ciocarlan, A.; Stoian, A. Ship Detection in Sentinel 2 Multi-Spectral Images with Self-Supervised Learning. *Remote Sens.* **2021**, *13*, 4255. [CrossRef]
49. Russian Tanker Falsifies AIS Data, Hides Likely Activity around Malta and Cyprus. Available online: https://skytruth.org/2022/12/russian-tanker-falsifies-ais-data-hides-likely-activity-around-malta-and-cyprus/?fbclid=IwAR1865fkOeoxP5h0arBYaSgtPQZw4AOXEvkr1ntMQ1IXTOJwqjf8U_iS6gk (accessed on 15 December 2022).
50. The Impact of Russia's Year-Long Invasion on the Maritime Ecosystem & Global Economy. Available online: https://www.hellenicshippingnews.com/the-impact-of-russias-year-long-invasion-on-the-maritime-ecosystem-global-economy/ (accessed on 15 February 2023).
51. How Russian oil Evades EU Sanctions and Land in European Ports. Available online: https://www.rferl.org/a/russia-ukraine-eu-oil-sanctions-shipping/32025726.html (accessed on 20 September 2022).
52. European Maritime Safety Agency. 19th Mediterranean AIS Expert Working Group Meeting—Report. EMSA Ref. Ares(2023)183539-11/01/2023. Available online: https://www.emsa.europa.eu/ssn-main/258-other-ssn-initiatives/4885-19th-mediterranean-expert-working-group-meeting.html (accessed on 15 December 2022).
53. Johnson, S.; Rachel, L.; Wolfram, C. Theory of Price Caps on Non-Renewable Resources. National Bureau of Economic Research. 2023. Available online: https://www.nber.org/system/files/working_papers/w31347/w31347.pdf (accessed on 23 September 2023).
54. The Laundromat: How the Price Cap Coalition Whitewashes Russian Oil in Third Countries. Available online: https://energyandcleanair.org/wp/wp-content/uploads/2023/04/CREA_The-Laundromat_How-the-price-cap-coalition-whitewashes-Russian-oil-in-third-countries.pdf (accessed on 8 May 2023).
55. Tsakiris, I. Bringing the 'Dark' Fleet into the Light. *IUMI EYE* **2023**, *40*, 15. Available online: https://iumi.com/news/iumi-eye-newsletter-march-2023/bringing-the-dark-fleet-into-the-light (accessed on 20 March 2023).
56. Michelle Wiese Bockmann: Shifty Shades of Grey: Dark Fleet Shipping Sanctioned Oil around the World. Available online: https://www.youtube.com/watch?v=-DH9XkwN3tY (accessed on 23 September 2023).
57. Geollect: Ship AIS Data Spoofed to Draw Pro-War Russian Z Symbol in Black Sea. Available online: https://lnkd.in/eug5qJVz (accessed on 25 May 2023).
58. Jarle Coll Blomhoff: Building Strong Cyber Security into Ship Design. Available online: https://www.dnv.com/expert-story/maritime-impact/building-strong-cyber-security-into-ship-design.html (accessed on 12 October 2023).