frontiers | Frontiers in Computer Science

TYPE Brief Research Report
PUBLISHED 14 August 2023
DOI 10.3389/fcomp.2023.1185760

Shining a light on AIS Blackouts with maritime OSINT

Emerald Cara Sage*

OSINT Combine, Sydney, NSW, Australia

OPEN ACCESS

EDITED BY
Stephen James McCombie,
NHL Stenden University of Applied Sciences, Netherlands

REVIEWED BY
Dusica Marijan,
Simula Research Laboratory, Norway
Adam Turner,
Macquarie University, Australia

*CORRESPONDENCE
Emerald Cara Sage
✉ emerald@osintcombine.com

RECEIVED 13 March 2023
ACCEPTED 06 July 2023
PUBLISHED 14 August 2023

CITATION
Sage EC (2023) Shining a light on AIS Blackouts with maritime OSINT.
Front. Comput. Sci. 5:1185760.
doi: 10.3389/fcomp.2023.1185760

Maritime open source intelligence (maritime OSINT) can be used to capture information, critical to business operations, including when electronic systems like Automatic Identification Systems (AIS) fail. AIS is used to identify vessels in maritime navigation, to plan shipping operations, and ensure safety. This data is collected and sold by global aggregators to maritime operators and industry stakeholders. However, AIS communications are vulnerable to malicious cyber activity, changing legal landscapes, adverse physical conditions, or intentional intervention. It is the latter we will focus on in this report. Often, we won't understand the motivation behind a decision to either switch off or manipulate AIS data. However, this decision can have real world impacts, including on relationships between nation states, and the physical safety of maritime personnel. We believe maritime OSINT may represent an effective method to assist in the management of AIS failures. Maritime OSINT not only captures important maritime information when AIS fails, but it provides valuable context, giving us the who, what, and why for vessel operations. In our cast study, we will use maritime OSINT to track sanctioned Russian oil exports, demonstrating how OSINT can be used in this example to inform sanctions compliance programs.

KEYWORDS

OSINT, OSINT techniques, maritime security, maritime safety, maritime governance

1. Introduction

1.1. Defining AIS

AIS uses the very high frequency (VHF) radio broadcasting system to transfer data. AIS equipped vessels and shore-based stations rapidly exchange identifying information about a vessel's identification, position, course, and speed (Australian Maritime Safety Authority, 2023). This information is crucial to ensure safe navigation and efficient operations, both during transit and whilst maritime vessels are in port. In 2000, the International Maritime Organization (IMO) stipulated that larger vessels were required to carry AIS capable of providing information about the vessel to other vessels and coastal authorities. The IMO stipulated that ships fitted with AIS had to ensure it remained operational at all times—with some very limited exceptions (International Maritime Organisation, 2023).

1.2. Implications of intentional AIS failures

AIS failures due to intentional intervention, occur for a variety of reasons and will continue to occur. These failures have real implications for global geopolitics, for aiding and abetting criminal activities, and for maritime safety (US Department of Transport Maritime Administration, 2023). Two recent examples of AIS intervention really underscore the implications of AIS failures.

In March 2021, a Swedish newspaper called "Dagens Nyheter," claimed AIS data for Nine Swedish Navy vessels incorrectly indicated they were conducting maneuvers in the Baltic Sea, specifically near the Russian city of Kaliningrad. Representatives from the Swedish Navy who were interviewed for the story, stated this AIS data has been falsified (Bergman, 2021). Researcher Bjorn Bergman, compared the AIS broadcasts associated with the incorrect vessel locations to genuine broadcasts from the same vessels. He found that the AIS broadcasts reporting the false positions had subtle differences to the genuine ones. Bergman concluded these AIS broadcasts had been deliberately falsified or "spoofed" (Bergman, 2021). Bergman found no direct evidence linking the false AIS broadcasts to a specific country, organization, or individual. However, he suggested they were consistent with Russian disinformation and spoofing tactics reported by multiple sources (Bergman, 2021; Herdt and Zublic, 2022). Although we may never know who spoofed this AIS data, the entity responsible effectively enflamed tensions in an otherwise volatile area.

AIS can be undermined by other vectors too, including nation-state legal requirements. In November 2021, the Government of the People's Republic of China (PRC) implemented the Personal Information Protection Law (Simplified Chinese: 中华人民共和国个人信息保护法). This legislation applies to organizations and individuals who process personally identifiable information belonging to Chinese citizens both within China and abroad. It includes strict requirements for data transfer, security controls, and data localization [Ken (Jianmin) and Jet (Zhizong), 2022]. As Chinese AIS land-based broadcasters worked out the implications of this legislation on their operations, there was a temporary land-based AIS blackout across China (LaRocco, 2021), endangering vessel operations in some of the busiest shipping routes in the world.

1.3. The importance of maritime OSINT

Although an important data source, AIS is just part of the rich and diverse information domain that we call maritime OSINT. Google searches using the terms "maritime OSINT" will often prioritize results linked to AIS data aggregators. These are corporate entities which collect AIS signals from multiple sea and land-based sources and then sell this data to shipping businesses and individuals. Google web crawling and ranking algorithms generate the impression that maritime OSINT is primarily generated by these AIS data aggregators. However, maritime OSINT is so much more. Our case study explores maritime OSINT as a capability that can be used to track sanctioned Russian oil exports, thereby informing sanctions compliance risk assessments.

1.4. Important maritime OSINT sources

1.4.1. The maritime OSINT domain

We use ***social media intelligence or SOCMINT*** to inform our understanding of shipping and port personnel. Identifying the people linked to vessels and shipping infrastructure can tell us about vessel ownership and associated supply chains. We can also use SOCMINT to identify links between shipping operations and adversarial, nefarious, or illegal activity. Soldiers, sailors, militiamen, and criminal syndicate members post pictures to social media which unintentionally show a landmark, or street sign which can be used to identify their location. Researchers and traditional media outlets also use social media profiles to post invaluable analysis of paid data, such as satellite imagery. By following these social media profiles, we can remain aware of the whereabouts of specific vessels of interest (Makowski, 2022).

When we are investigating maritime linked supply chains, ***company related data*** is an important source of information. Vessels are often owned, operated, and repaired by different companies. Many maritime companies are in fact shell companies, used to obfuscate the real owners or operators of a particular vessel. Shell companies are used to circumvent sanctions, evade financial restrictions, or hide nefarious and illegal activity from law enforcement agencies. ***Sanctions data*** is therefore another important part of the maritime OSINT domain (Wondersmith_Rae, 2022).

Lastly, and perhaps most importantly we use ***mapping applications, satellite imagery, webcam footage, and photos*** to identify a vessel's location, provide insight into a port's environment and the activities occurring there. On video sharing sites like YouTube, you can find videos tagged to specific locations that give you visual insights into a vessel's interior environment, its onboard operations, and personnel. In our case study we demonstrate how you can use webcam footage and photos uploaded to social media to identify and monitor vessels entering Russian oil ports.

2. Methodology

This paper demonstrates the utility of OSINT to the continuity of maritime operations, particularly when electronic information collection systems fail. We identified the principal entities driving maritime operations—these being people, companies, and vessels—then applied freely available OSINT tools and techniques to acquire information about these entities. The OSINT tools and techniques used were selected against the following criteria: (a) used legitimate and ethically sourced data; (b) were reliable; (c) were publicly available; and (d) were low cost, or free. These criteria ensured the OSINT tools and techniques used were a viable option for anyone working in maritime operations.

Research on the applicability of OSINT to maritime operations has been limited. Only one other author (Baker, 2023) has systematically reviewed OSINT tools and techniques for maritime related operations and investigations. This author has generated a vast body of work, including catalogs of OSINT tools and techniques applicable within a maritime context, and multiple specific use cases. Our findings are consistent with the conclusions drawn by this author—OSINT is immensely useful within various aspects of the maritime domain.

For the purposes of our research, we sought to test the value of the information obtained, by applying our methodology to a specific use case. We looked at people, companies, and vessels involved in sanctioned Russian oil exports and sought to determine if our findings provided sufficient information to inform sanctions compliance program evaluations. We found that freely available

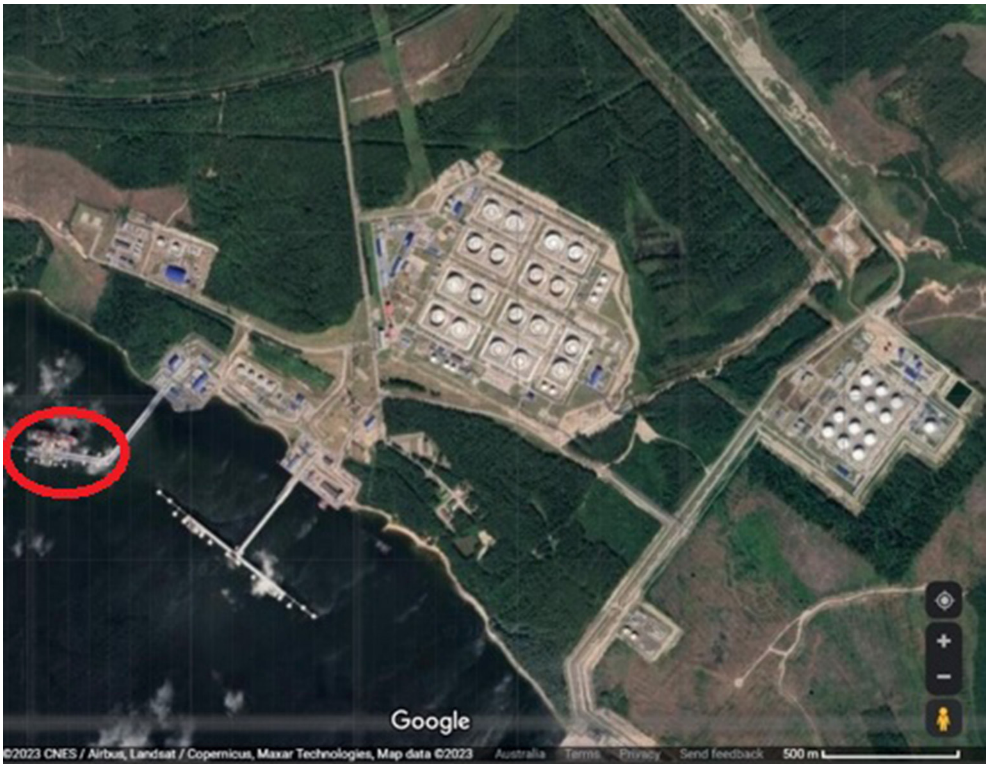

Google
©2023 CNES / Airbus, Landsat / Copernicus, Maxar Technologies, Map data ©2023 Australia Terms Privacy Send feedback 500 m

FIGURE 1
Google satellite imagery of the Port of Primorsk in Russia. This imagery was captured on an unknown date in 2023.

OSINT tools and techniques identified a vessel being used to covertly export Russian oil. This vessel therefore represented a risk to sanctions compliance programs.

3. Discussion and case study

3.1. A brief overview of Russian oil sanctions

In response to the conflict in Ukraine, European Union (EU) nations have issued sanctions ending imports of Russian oil by sea (The Economist, 2022). In addition, some nations have set a price cap on Russian seaborne crude oil, which prohibits the use of Western-supplied maritime insurance, finance, and other services unless the Russian crude is sold below $60 USD per barrel (Horton and Palumbo, 2023). Tracking the export of Russian oil, particularly if it goes above $60 USD per barrel will be critical for sanctions compliance programs across the western world.

When exporting Russian oil, some vessels have been observed switching off their onboard AIS (Towey, 2022). Disabling or manipulating AIS makes it hard for governments to track vessels exporting Russian oil. It also represents a risk to private enterprise through unintentional exposure to sanctioned entities in supply chains and through trade. We believe ship owners, ship managers, ship operators, brokers, flag registries, port operators, freight forwarders, commodity traders, insurance companies, and financial institutions, can use maritime OSINT to appropriately assess their sanctions risk by determining whether Russian oil is in their supply chain.

3.2. Using maritime OSINT to track Russian oil exports

3.2.1. Using satellite images

Three ports process most of Russia's crude and refined oil exports. These are: Primorsk, Novorossiysk, and Ust-Luga (US Energy Information Administration, 2023). Google or Yandex satellite images (Yandex is a Russian Google equivalent) can provide insights into the primary function of port operations. In Figure 1, we can see a series of oil storage structures adjoining the piers, confirming this port is likely used to export oil. When we increase the resolution ships are legible. A ship docked at the Port of Primorsk, Russia, is highlighted by a red circle in Figure 1. Some maritime researchers with expertise in tanker architecture can use these images to identify vessels. However, it can be hard to verify any assessments made as the satellite imagery doesn't offer an exact date, and the aerial perspective makes it difficult to view details such as names, and International Maritime Organization (IMO) ship identification numbers. There are mapping services like NASA's Worldview which allow us to view satellite imagery captured on specific dates, but the resolution often makes identification based on small visual features difficult, and it doesn't solve the issue of visual perspective.

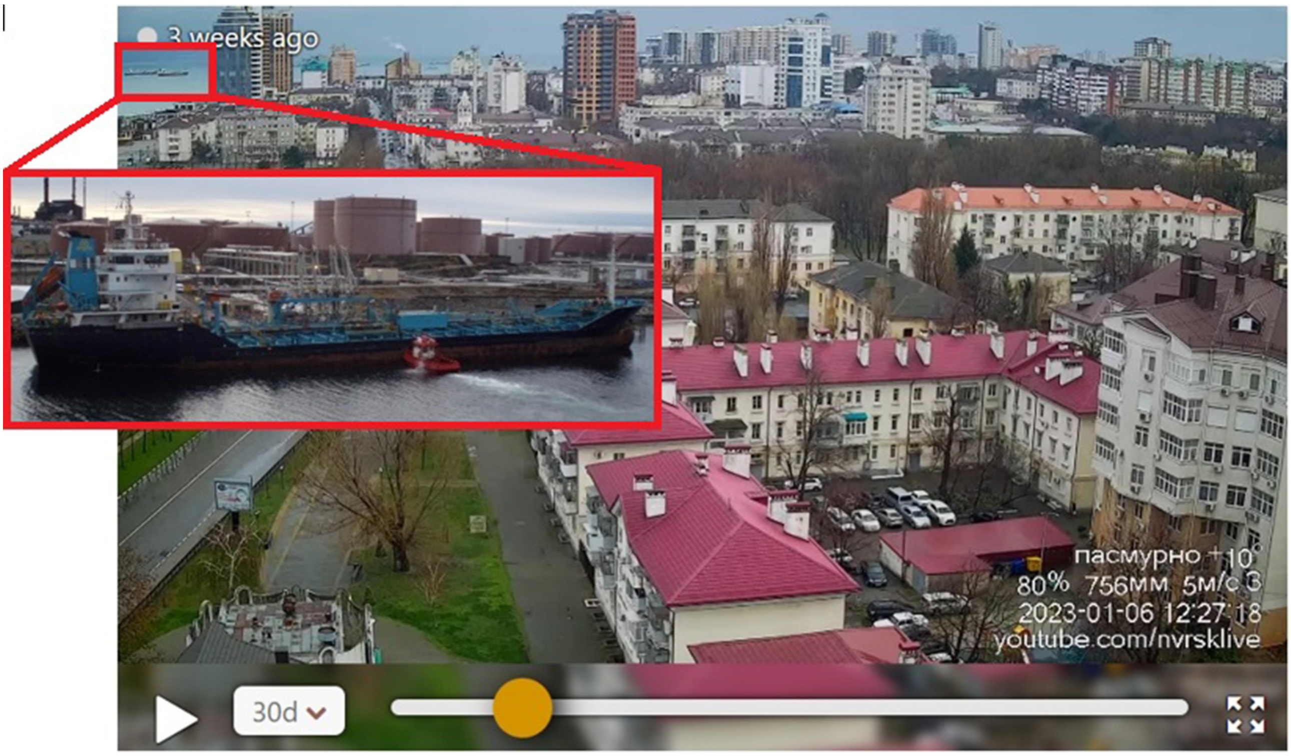


FIGURE 2
Webcam footage taken from Windy.com on 6 January 2023, showing the Port of Novorossiysk in Russia. Two ships can be seen traversing waters in close proximity to the Port.

3.2.2. Satellite imagery of the Russian port of primorsk

3.2.2.1. Using webcams

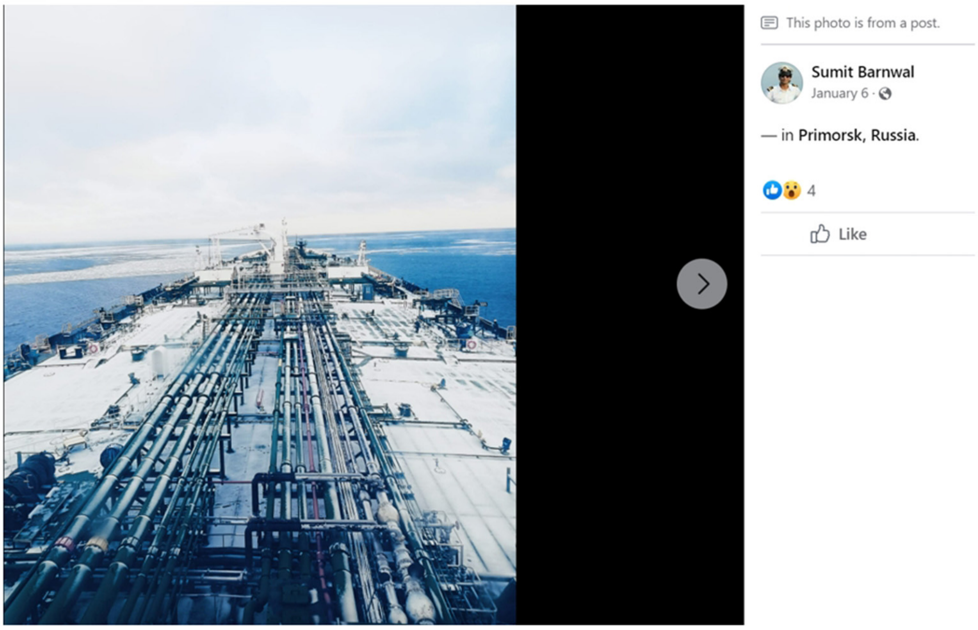
We can use webcam footage of specific locations using different tools and online platforms. Websites like Windy.com offer free access to webcams placed across the world, allowing users to monitor real time weather conditions and fluctuations in weather patterns over time. A Windy.com webcam was identified at the Port of Novorossiysk. With image editing software it is possible to view the oil vessels transiting a specific section of the port as seen in Figure 2. Using large scale visual markers and comparing these to images of ships which may have been reported in the area, we can potentially identify these ships.

In Figure 2, one of the vessels in the top left is colored blue and white. It also had what appears to be a raked shape bow, and pinnacle antennae design. Although there are many ships with these visual characteristics, we can use a photo sharing platform like shipspoting.com and filter photos by categories like "home port." In this case we filtered by the Port of Novorossiysk and found the Ivan Poddubny, which looks visually similar to one of the ships captured in the windy.com webcam footage.

When using OSINT, it is good practice to verify or validate information by comparing the original source of this information to other sources of the same information or reporting. The maritime website fleetmon.com provides users with access to a port database which displays specific details for global ports including weather, usage, vessels, and media reporting. Although the database includes AIS, it supplements AIS with additional data sources allowing users to validate and corroborate AIS within the one platform. When we searched the port of Novorossiysk, we found five large vessels had been spotted in this port on the date the webcam footage was taken. One of these vessels was the Ivan Poddubny. We can therefore assess one of the ships captured in the webcam footage could be the Russian-owned and operated vessel, the Ivan Poddubny. We can therefore infer that the Ivan Poddubny is potentially being used to transport and/or export Russian oil. We may therefore wish to continue monitoring the Ivan Poddubny as we continue to monitor sanctioned Russian oil exports.

3.3. Using SOCMINT

Webcam services like windy.com do not necessarily cover all the world's ports. Where we want to look at ships visiting a port not covered by webcam footage, we can search for images tagged to these port locations on social media platforms like Facebook. In the example below, we conducted a search across Facebook using the word "ship" and filtered photos by the tagged location: "Primorsk,



This photo is from a post.

Sumit Barnwal
January 6 ·

— in Primorsk, Russia.

4

FIGURE 3
Post made to the Sumit Barnwal Facebook profile on 6 January 2023. This post includes a photo of the deck of a shipping vessel.

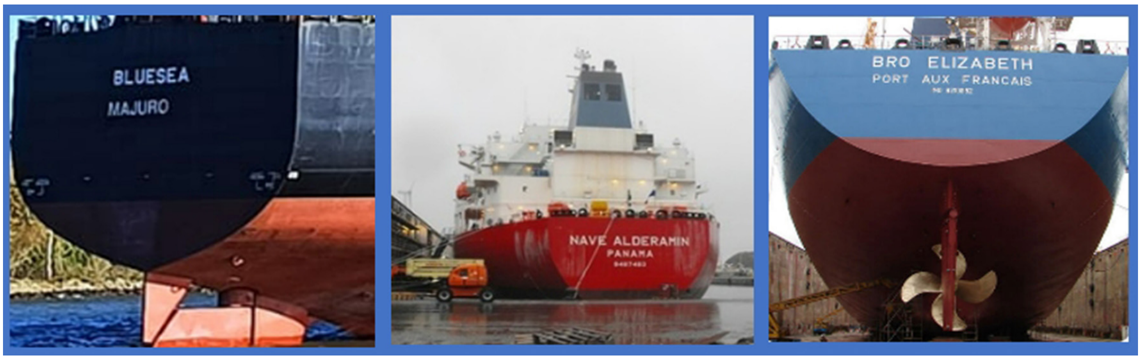


FIGURE 4
The "stern" or aft-most part of three vessels. Far right is the "Bluesea" which lacks an IMO number. Images in the center and far right show registered vessels with standard name and IMO labeling.

Leningradskaya Oblast, Russia." We retrieved an image uploaded to Facebook on 6 January 2023, by the user "Sumit Barwal." This image shows what appears to be the deck of a large shipping vessel, and features shown are consistent with images taken at this angle of oil tanker vessels (see Figure 3) (Facebook, 2023).

When we viewed this user's Facebook profile information, we found he had disclosed his profession as: "engineer officer at Shipping Corporation of India Ltd." Looking through his posts we found he had uploaded a photo of a vessel tagged to the "Gulf of Mexico" on 19th December 2022 (Facebook, 2023).

The physical dimensions of this vessel are similar to the image of the vessel's forward deck uploaded to the same Facebook account and tagged to Primorsk. We could view letters on the back of the ship which spelt the name "Bluesea" and the Port "Majuro" underneath (see the image of the ship on the far left in Figure 4). We searched across ship ownership databases and failed to find any records of a ship under this name with the same structural characteristics. In their advisory of 2020, The US Government stated vessels involved in illicit activities had altered physical identification markers by painting over vessel names and IMO numbers [US Government Sanctions Advisory (2020)]. It is possible the vessel pictured above has had its physical identification markers altered.

This theory has plausibility when we look at valid and verifiable examples of how names and IMO numbers are generally painted on legitimately registered ships of this category, and then compare these with the "Bluesea." When we do this, we find the "Bluesea" lacks detail like an IMO number, and the placement of the name and port reference are off center as shown in Figure 4.

The user of the Sumit Barwal Facebook profile had uploaded multiple photos of himself aboard what appears to be the same large vessel and tagged these photos to multiple locations over time. Using this information, we were able to plot his movements during the period 19th December 2022 to 27th January 2023 without AIS data (Facebook, 2023).

Furthermore, using his Facebook name and images, we were able to retrieve an Instagram (Instagram, 2023) and Twitter (Twitter, 2023) account under the same name with an identical profile picture. Another photo posted to the Sumit Barwal Twitter account (Twitter, 2023) showed the user wearing a name badge which read: "Sumit Kumar." This suggests the user may have created his social media profiles under an alias. It also provides us with additional names to search should we wish to identify this individual.

3.4. Using company data

Data aggregators like Dun&Bradstreet and OpenCorporates, have access to information provided by individuals when they register a business or organization. Some governments, like the Government of the PRC, restrict the sale of sovereign company data. A nil search result therefore doesn't necessarily indicate there is nothing to find. If we know an entity is linked to a country with extensive data protection legislation, we can go directly to indigenous company data repositories, or Government provided search engines.

In our example, a search across Dun&Bradstreet using the company name: "Shipping Corporation of India Ltd" found records for a company with a tiered corporate structure spread across India, the United Kingdom, Singapore, and Belgium. Looking at records for the parent company we were able to retrieve a company address, a key principle (key individual associated with the company's registration), and a website. A review of the company website located a list of the company's fleet. We found 13 vessels used to transport crude oil and none bore the name "Bluesea".

We also found a link to the company's annual corporate reports. A review of the corporate report for 2020–2021 identified members of the board of directors, and major shareholders.

3.5. Searching across sanctions data

OpenSanctions.org is a data aggregator for sanctioned entities. Their database includes holdings from multiple governments and organizations including the European Union (EU). We used the OpenSanctions.org search engine to check "Shipping Corporation of India Ltd" and the oil tankers listed on the company website. These searches failed to return any results. We then started to search for shareholders referenced in the annual report. We found a shareholder named "BIIS Maritime Limited" had been sanctioned for being a subsidiary of "Irano Hind Shipping Co" - an Iranian shipping company exporting sanctioned commodities including oil from Iran.

Another technique we used to retrieve corporate connections linked to sanctioned entities was to query data collected and published online by investigative journalists. The Organized Crime and Corruption Reporting Project (OCCRP) supported by the Google Digital News Initiative, have developed a tool called "Aleph." This tool allows users to search across multiple databases, including those linked to the "Panama Papers" and curate search findings into graphs, tables, and charts to highlight linkages. Offshore Leaks is another service like OCCRP's Aleph. Founded by the International Consortium of Investigative Journalists, this service has access to an extensive repository of data from 200 locations. Using a combination of these tools and data repositories we were able to identify multiple additional entities linked to "Irano Hind Shipping Co," gradually building out the Shipping Corporation of India Ltd supply chain.

3.6. AIS data

We used AIS data aggregators VesselFinder.com and MarineTraffic.com to search for arrivals at the Port of Primorsk on 6 January 2023. We were unable to identify any of the ships listed on the Shipping Corporation of India Ltd website, or any records of the "Bluesea." We amended our search criteria to include a 7-day period both before and after 6 January 2023, which still returned no results. These findings suggest the vessel carrying the Facebook user "Sumit Barwal" either switched off or spoofed it's AIS and/or arrived in Primorsk under a different name to obfuscate its identification.

4. Conclusion

Using Maritime OSINT in our case study we were able to identify a Russian vessel likely used to transport crude oil (the Ivan Poddubny). Although basic Google searches indicate this vessel is an oil tanker, using Maritime OSINT we found this vessel is likely still operating, including through the Port of Novorossiysk. Through our case study, we were also able to identify another vessel possibly linked to an Indian company trading with sanctioned entities and commodities. This vessel appeared to have docked at the Russian oil port of Primorsk and failed to use AIS when doing so. Based on our findings we can surmise that it is possible the "Bluesea" is being used to covertly export Russian oil. Based on these findings we would continue to monitor these vessels which both represent a risk to sanctions compliance programs.

Our case study also clearly demonstrates maritime OSINT is more than AIS data. It is a versatile and powerful resource for operators working in the maritime domain. We have demonstrated tools and techniques which are effective, but not proscriptive. Most OSINT tools and techniques can be applied in a variety of different ways to various information requirements.

It's also important to note the OSINT landscape is constantly changing. As new platforms and technologies become available more effective and efficient tools emerge. OSINT is also impacted by forces such as changes in people's online behavior and data privacy legislation. A key component of maritime OSINT is remaining attuned to these changes and finding ways to adapt when they occur.

Data availability statement

The original contributions presented in the study are included in the article/supplementary material, further inquiries can be directed to the corresponding author.

Ethics statement

Written informed consent was not obtained from the individual(s) for the publication of any potentially identifiable images or data included in this article.

Author contributions

The author confirms being the sole contributor of this work and has approved it for publication.

Conflict of interest

The author declares that the research was conducted in the absence of any commercial or financial relationships that could be construed as a potential conflict of interest.

Publisher's note

All claims expressed in this article are solely those of the authors and do not necessarily represent those of their affiliated organizations, or those of the publisher, the editors and the reviewers. Any product that may be evaluated in this article, or claim that may be made by its manufacturer, is not guaranteed or endorsed by the publisher.

References

Australian Maritime Safety Authority (2023). About the automatic identification system. Available online at: https://www.amsa.gov.au/safety-navigation/navigation-systems/about-automatic-identification-system (accessed February 3, 2023).

Baker, R. (2023). *Deep Dive: Exploring the Real-World Value of Open Source Intelligence*. Hoboken, NJ: Wiley and Sons Inc.

Bergman, B. (2021). *Systematic Data Analysis Reveals False Vessel Tracks*. Shepherdstown, WV: Sky Truth. (accessed February 3, 2023).

Facebook (2023). Available online at: https://www.facebook.com/sumit.sumit.485. (accessed February 3, 2023).

Herdt, C. S., and Zublic, M. (2022). *Baltic Conflict: Russia's Goal to Distract NATO?* Washington, DC: Centre for Strategic and International Studies (accessed February 3, 2023).

Horton, J., and Palumbo, D. (2023). *Russia Sanctions: What Impact Have They Had on Its Oil and Gas Exports*? London: BBC News Service (accessed February 3, 2023).

Instagram (2023). online at: https://www.instagram.com/p/CmUswvqsaBM/. (accessed February 3, 2023).

International Maritime Organisation. (2023). Regulations for carriage of AIS. Available online at: https://www.imo.org/en/OurWork/Safety/Pages/AIS.aspx (accessed February 3, 2023).

Ken (Jianmin), D., and Jet (Zhizong), D. (2022). *China's Personal Information Protection Law (PIPL)*. Bloomberg Law.

LaRocco, A. (2021). *Latest Supply Chain Challenge: China's Terrestrial AIS Data Blackout*. Chattanooga, TN: Freight Waves (accessed February 3, 2023).

Makowski, M. (2022). *The Power of Maritime OSINT—Interview with Wondersmith Rae*. Warsaw: eForensics Magazine (accessed February 3, 2023).

The Economist (2022). *How Russia Dodges Oil Sanctions on An Industrial Scale*. London: The Economist. (accessed February 3, 2023).

Towey, H. (2022). *Russian Tankers Turned Off Their Tracking Signals at More Than Double the Normal Rate in March, as 'Dark Activity' Skyrockets Following the Invasion of Ukraine*. New York, NY: Business Insider. (accessed February 3, 2023).

Twitter. (2023). Available online at: https://mobile.twitter.com/Sumit6913 (accessed February 3, 2023).

US Department of Transport and Maritime Administration (2023). "2022-005-Various-GPS Interference and AIS Spoofing." Available online at: https://maritime.dot.gov/msci/2022-005-various-gps-interference-ais-spoofing (accessed February 3, 2023).

US Energy Information Administration (2023). "U.S. Energy Information Administration, International Energy Statistics and BP's Statistical Review of World Energy 2022". Available online at:https://www.eia.gov/international/content/analysis/countries_long/russia/#:$\sim$:text=Four%20ports%20Primorsk%2C%20Nakhodka%2C,product%20exports%20(Table%205) (accessed February 3, 2023).

US Government Sanctions Advisory (2020). U. S. Department. of the Treasury, Department of State, United States Coast Guard. (2020). "Guidance to Address Illicit Shipping and Sanctions Evasion Practices." Available online at: https://home.treasury.gov/system/files/126/05142020_global_advisory_v1.pdf (accessed February 3, 2023)

Wondersmith_Rae (2022). "Maritime OSINT: Port Analysis". Available online at:https://wondersmithrae.medium.com/maritime-osint-port-analysis-d09b4531728d. (accessed February 3, 2023).

Free Maritime OSINT Tools

Company Data

DunandBradStreet: https://www.dnb.com
OpenCorporates: https://opencorporates.com/
ZoomInfo: https://www.zoominfo.com/
MarketScreener: https://www.marketscreener.com/
LinkedIn: https://www.linkedin.com/
Wallmine: https://pl.wallmine.com/
Offshore Alert: https://www.offshorealert.com/
US Government (OFAC) Sanctions Search:
https://sanctionssearch.ofac.treas.gov/
Offshore Leaks: https://offshoreleaks.icij.org/
OCCRP Aleph: https://aleph.occrp.org/search
Global Sanctions Search: https://www.opensanctions.org/

Imagery

Webcams: https://www.windy.com/
Google Satellite: https://www.google.com/maps
Yandex Satellite: https://yandex.com/maps/
NASA Satellite imagery: https://worldview.earthdata.nasa.gov/
ESRI: https://www.esri.com/
SOAR: https://soar.earth/
OpenStreetCam: https://kartaview.org/
OpenStreetMap: https://umap.openstreetmap.fr/

Vessel/Port Identification

ShipSpotting: https://www.shipspotting.com/
MarineTraffic: https://www.marinetraffic.com/en/ais/home/centerx:-12.0/centery:25.0/zoom:4
VesselFinder: https://www.vesselfinder.com/
Ports Database: https://www.fleetmon.com/
FleetMon: https://www.fleetmon.com/
ShipFinder: https://shipfinder.co/
AllTrack: https://alltrack.org/
AISHub: https://www.aishub.net/
MarineOnline: https://www.marineonline.com/