7

Vessel-Tracking Innovations

Promise and Peril

Richard L. Kilpatrick, Jr.

7.1 INTRODUCTION

Maritime law enforcement initiatives are increasingly dependent on tracking vessel movements at sea. Although some vessel operators engaged in nefarious activities – such as contraband trafficking, economic sanctions circumvention, piracy, and illegal fishing – attempt to operate without regulatory oversight, authorities are tapping into emerging technologies as a means of exposing those activities.[1] Running parallel to enforcement actions, regulators are also obliging legitimate commercial shipping participants to enhance compliance initiatives, which is further building reliance on sophisticated vessel-tracking products developed by third-party technology companies.[2] These innovations repackage vessel-tracking data collected to promote maritime safety and achieve search-and-rescue preparedness into computer applications that provide actionable recommendations designed for compliance monitoring. Notably, many of these market-leading vessel-tracking tools rely on Automatic Identification System (AIS) transmissions flowing from treaty obligations designed to protect the safety of life at sea.[3] By processing this data with cutting-edge advances in machine learning, advanced algorithms, and artificial intelligence, and cross-referencing this information with other sources of vessel location data, such as real-time high-resolution satellite imagery, vessel-tracking companies are offering regulatory authorities and compliance-attuned commercial actors the tools necessary to embrace a new era of maritime transparency.

[1] Other unlawful activities recently revealed by vessel-tracking technology include undersea cable sabotage and cargo laundering (Bockmann 2024a; Diakun 2023b; Lloyd's List 2025).

[2] The IMO has recently highlighted the safety, security, and environmental consequences of a "dark fleet" of vessels attempting to sidestep oversight by "intentionally taking measures to avoid ship detection" (IMO 2023).

[3] For instance, many of the vessel-tracking products rely substantially on the location transmissions flowing from compliance with the International Convention for the Safety of Life at Sea, November 1, 1974, 1184 UNTS 2, as amended (SOLAS 1974).

https://doi.org/10.1017/9781009760171.013 Published online by Cambridge University Press

Public authorities are relying on these innovations to maintain maritime domain awareness as criminal actors double down on efforts to disguise their activities. Simultaneously, legitimate commercial actors are deploying these transparency tools both to match due-diligence obligations imposed by regulators and to protect themselves in the commercial disputes that flow from exposure to noncompliance. In this way, recent innovations in vessel tracking are serving multiple purposes: to strengthen law enforcement initiatives and to serve as commercial intelligence for legitimate actors aiming to avoid penalties, protect against contractual liabilities, and guard against the reputational harm associated with unlawful trades. But as vessel-tracking technology improves, this is also increasing the risks for the misuse of sensitive vessel location information. Just as enhanced vessel-tracking technology may be used for the commendable purposes of promoting the safety of life at sea, facilitating law enforcement initiatives, and bolstering private sector compliance efforts, the same information may also be commandeered by malign actors to target merchant vessels for piracy or politically motivated attacks. The risks associated with sophisticated vessel tracking are now starkly illustrated by the many recent attacks against merchant ships performed by Houthi militants occupying parts of Yemen. As merchant vessels have attempted to transit the Baab Al-Mandab Strait and the Red Sea for access to the Suez Canal, the Houthis have repeatedly targeted vessels after engaging in intelligence gathering of the vessels' trading histories and ownership links.[4] This alarming trend highlights the need to prevent emerging vessel-tracking technology from being abused by hostile actors (Mathews 2024; Sweeney 2024).

Examining that dichotomy of transparency and risk, this chapter explores the technological, strategic, and policy evolutions that developed over decades of monitoring vessel movements through technology. First, the chapter maps the evolving stages of vessel-tracking tools from the invention of the radio in the nineteenth century, to the treaty-mandated equipment and satellite-supported framework developed incrementally during the twentieth century, and finally to the technology-fueled present. It then explores the shifts that led to the tools originally adopted for the safety of life at sea to be repurposed into law enforcement and compliance mechanisms and analyzes how this approach has spawned unexpected vulnerabilities. Finally, the chapter discusses the future of vessel tracking by framing the emerging tools as critical to enhancing maritime transparency while also generating new responsibilities to counteract resulting risks.

7.2 VESSEL TRACKING: PAST, PRESENT, AND FUTURE

7.2.1 *Radio to GMDSS*

Before the advent of radio technology, ships operating at sea relied on visual and audible methods to signify their locations to other ships and to shore. Shipmasters

[4] These Houthi attacks on commercial shipping have been condemned by the UN Security Council (UNSC 2024a, 2024b).

https://doi.org/10.1017/9781009760171.013 Published online by Cambridge University Press

and crews were confined to using rudimentary tools, such as flags, lamps, and flares, or bells, horns, and whistles, to communicate with other vessels and to shore for safety-of-navigation purposes and in the event of distress situations. These limitations substantially impacted the ability to react in the event of a maritime emergency demanding assistance. The invention of the radio during the late nineteenth century revolutionized opportunities for maritime communication that could span much longer distances. Equipping vessels with radio transmitters and antennas made it possible to transmit telegraphic messages through Morse code for many miles. During the early twentieth century, this radio technology was incorporated into the technical machinery of some ships, but this was not yet compulsory. In efforts to harmonize the use of the equipment and the communications methods, more than twenty nations agreed in 1906 to an International Radiotelegraph Convention[5] outlining commitments regarding radiotelegraph processes, including for maritime distress situations.

A technological leader in the field at the time was the Marconi Company, established by Italian inventor Guglielmo Marconi (Baker 1971). The Marconi Company outfitted many ships with equipment during the early twentieth century, including the infrastructure on the RMS *Titanic*, which had its own "Marconi Room" (Photo Museum Ireland n.d.). During the *Titanic*'s ill-fated voyage in 1912, Marconi Company technicians sent telegraphic messages on behalf of passengers as the vessel made its way from Southampton toward New York (Hersey 2012). After the vessel hit an iceberg hundreds of miles from the coast of Canada, the same radio technicians relayed a distress message, "CQD," which was received by several ships, resulting in a rescue response saving hundreds of passengers.[6] But more passengers may have been saved had there been a more coordinated response by additional vessels nearby.

The *Titanic* disaster mobilized significant changes in the way that ships at sea utilized radio technology to aid safe navigation, as the incident quickly led to international efforts to incorporate radio technologies into regulatory mandates. The 1914 Convention for the Safety of Life at Sea (SOLAS 1914)[7] codified for the first time an obligation for merchant shipmasters to monitor designated radio channels for distress alerts that might be relayed by nearby vessels. SOLAS 1914 required qualifying ships to be fitted with a "radiotelegraphic installation" capable of "clearly sending perceptible signals" covering at minimum 100 sea miles (Articles 31 and 35).

As innovations expanded, especially during the two World Wars, these tools were incorporated into new efforts to facilitate maritime safety on a global scale.[8] This was

[5] International Radiotelegraphic Convention, November 29, 1906.

[6] "CQD" was understood at the time to mean roughly "all stations distress." It was a form of distress message equivalent to "SOS" (*New York Times* 1912).

[7] Convention for the Safety of Life at Sea, January 20, 1914 (SOLAS 1914).

[8] SOLAS was updated in 1929 to reflect technological changes occurring during and after the First World War: International Convention for the Safety of Life at Sea, May 31, 1929, 136 LNTS 81.

https://doi.org/10.1017/9781009760171.013 Published online by Cambridge University Press

aided by the postwar emergence of multilateral institutions, which provided the diplomatic infrastructure for negotiations of new treaties. In particular, the Intergovernmental Maritime Consultative Organization, the precursor to the International Maritime Organization (IMO), paved the way for the treaty-based measures designed to harmonize mandatory navigation information to be relayed and received by ships operating at sea (IMO n.d.). The advent of new space-based satellite equipment during the Cold War substantially strengthened these efforts as it became possible to relay radio messages by bouncing signals off satellites in continuous orbit, which enlarged the capability of sending and receiving distress messages from ships at sea, even those operating in remote locations.[9]

Incorporating these technological advancements, SOLAS was updated multiple times during the twentieth century.[10] The most recent wholesale revisions, reflected in SOLAS 1974,[11] contain explicit requirements for qualifying ships to utilize maritime monitoring equipment to facilitate data exchange and enhance communication between ships and to shore. SOLAS 1974 provisions required qualifying vessels to carry radio equipment capable of sending and receiving distress alerts across very-high-frequency (VHF) radio channels (Chapters IV–V). These included specific "shipborne navigational equipment," including various technologies of the era, such as radar and echo-sounding devices.

But telecommunications developed quickly in the years following SOLAS 1974, especially due to widespread advancements in satellite and space-based infrastructure. The SOLAS 1974 framework required further amendments to operationalize these technological developments. Having foreseen the likelihood of this need, the drafters of SOLAS 1974 included a flexible amendment procedure that allowed the IMO's Maritime Safety Committee (MSC) to update its provisions. In the following decades, fast-tracked changes facilitated regulatory dynamics to keep pace with evolving technologies (Article VIII).[12]

Among the most significant of the IMO's amendments to SOLAS 1974 is the establishment of the Global Maritime Distress and Safety System (GMDSS) in 1988 (Chapter IV, Regulation 4). The GMDSS amendments require qualifying ships to carry certain types of radio equipment that are capable of transmitting and receiving distress alerts and, at the push of a button, communicating a preformatted distress message to rescue coordination centers managed by State authorities (Bréhaut 2013). This GMDSS technology mandate requires the use of shipborne equipment

[9] These technological developments drove the establishment of an international framework governing the use of satellites to support maritime safety initiatives. See Convention on the International Maritime Satellite Organization, September 3, 1976, 1143 UNTS 105.

[10] For example, the International Convention for the Safety of Life at Sea, June 17, 1960, 536 UNTS 27.

[11] International Convention for the Safety of Life at Sea, November 1, 1974, 1184 UNTS 2 (SOLAS 1974).

[12] Under Article VIII of SOLAS 1974, amendments may be "referred to the Maritime Safety Committee of the Organization for consideration."

https://doi.org/10.1017/9781009760171.013 Published online by Cambridge University Press

designed to interact with satellites and shore-based tools to create a comprehensive long-distance messaging framework.[13] The advent of the GMDSS was a revolution in the development of international legal rules governing vessel tracking. By mandating satellite-linked transmissions covering even remote sea areas, the GMDSS created a new apparatus to protect life at sea by delivering critical vessel location information to State-operated rescue coordination centers prepared to react promptly to distress alerts.[14]

7.2.2 *AIS and LRIT*

This GMDSS framework paved the way for enhanced vessel tracking after the turn of the new century. In 2000, the MSC adopted further amendments to SOLAS to enhance navigational safety through the use of automatic information exchanges relayed via shipborne equipment (IMO 2000b). These SOLAS amendments require qualifying vessels to carry AIS equipment, which continuously relays identifying information on a VHF radio band, including the vessel's identity, type, position, course, speed, and navigational status, along with other safety information.[15] This information transmitted from the AIS equipment is then collected by other ships' receivers and by shore-based facilities for the purpose of promoting the underlying interests driving the SOLAS framework – namely, the safety of life, the safety of navigation, and the protection of the marine environment.

Shortly after the AIS mandate was promulgated, the MSC issued Guidelines for the Onboard Operational Use of Shipborne Automatic Identification Systems (AIS Guidelines; IMO 2001). The Guidelines, which were updated in 2015 to clarify further its implementation (IMO 2015), explain that the AIS should relay static information, such as the vessel's IMO number, Maritime Mobile Service Identity number, and details regarding its type and size. In addition, the AIS should also include "dynamic" information, such as the vessel's position, speed, and intended destination (IMO 2015). Some of this information, such as the vessel's position and speed, is updated automatically by the equipment, but other information, such as the vessel's destination, requires manual input (IMO 2015).[16]

Both the SOLAS amendments establishing AIS and the AIS Guidelines make it clear that operators of qualifying vessels have an obligation to relay the AIS information continuously. Thus, the AIS "should always be in operations when ships are

[13] In particular, the GMDSS rules mandate vessels carry emergency position indicating radio beacons, search-and-rescue transponders for precise location determination, and navigational telex devices that allow for the automatic reception of safety messages (USCG n.d.).

[14] This GMDSS also ties into the rescue framework established by the International Convention on Maritime Search and Rescue, April 27, 1979, 1405 UNTS 97.

[15] This qualification depends on the vessel's gross tonnage and whether the vessel is "engaged on international voyages." See SOLAS 1974, as amended, Chapter V, Regulation 19.

[16] For a visual description of AIS functionality, see NATO (2021).

https://doi.org/10.1017/9781009760171.013 Published online by Cambridge University Press

underway or at anchor" (IMO 2015). However, the Guidelines do indicate an important exception to this rule: "If the master believes that the continual operation of AIS may compromise the safety or security of his/her ship or where security incidents are imminent, the AIS may be switched off" (IMO 2015). In such unique security situations, the AIS Guidelines indicate that "the master should however restart the AIS as soon as the source of danger has disappeared" (IMO 2015).

The AIS requirement and its narrow security-based exception represent a critical moment in international regulation through vessel tracking, as the rules mandate continuous location and identity disclosures in the interests of safety at sea. But even at the time the rules were drafted, this transparency mandate and security exception was viewed as a necessary compromise. During the development of the AIS Guidelines, shipping industry organizations, including the International Chamber of Shipping (ICS) and the International Association of Independent Tanker Owners (INTERTANKO), expressed concern that the regulatory obligation requiring vessel operators to relay vessel locations continuously could ultimately create security risks. Although the ICS and INTERTANKO both submitted documents to the MSC in support of the adoption of the AIS requirements, the submissions also advocated for the shipmaster to retain the authority to turn off the transponder if the shipmaster believes that the safety of the ship could be affected by the transmission of its location (IMO 2000a, 2000c). This advocacy appears to have shaped the rule allowing shipmasters to switch off the AIS transponder at their discretion in the interests of maritime security.

An additional vessel-tracking amendment was made to SOLAS as part of a maritime security response to the 9/11 attacks. At that time, there was an urgent concern about the security vulnerabilities of maritime ports, which drove substantial regulation under IMO auspices, most notably the establishment of the International Ship and Port Facility Security Code (SOLAS 1974, Chapter XI; IMO 2012). In addition to these changes, to enhance vessel-tracking capabilities, the MSC updated SOLAS in 2006 to establish a Long-Range Identification and Tracking (LRIT) system to be carried out alongside the AIS requirements (IMO 2006). In some ways, the LRIT framework is similar to AIS and perhaps even redundant, but LRIT contrasts with AIS in that it relies on different technologies to relay a narrow scope of identifying information to a limited class of authorized audiences.[17]

The LRIT regulations require the automatic transmission of information: the ship's identity and position, along with the specific date and time of the messages (IMO 2006). The framework envisions the communication of vessel location data utilizing the same equipment already carried on ships to facilitate the original GMDSS program to cooperate with orbiting satellites and data collection facilities on shore (IMO 2006). Collectively, the equipment allows these tracking messages to be automatically relayed via a "digital select calling" process at six-hour intervals

[17] For a discussion of the policy arguments for the adoption of LRIT, see Krajewski (2008).

https://doi.org/10.1017/9781009760171.013 Published online by Cambridge University Press

without any human intervention or manual inputs (IMO 2006). This information is collected by designated service providers and then sent to authorized State organizations entitled to review the data – namely, flag, port, and coastal States that may wish to use the information to enhance search-and-rescue capabilities and to establish maritime domain awareness (IMO 2006). Even with transparency and security driving the adoption of the LRIT, under its framework, governmental entities accessing this data must "recognize and respect the commercial confidentiality and sensitivity" of the information they receive (IMO 2006). Thus, the distribution of LRIT data is much more confined than its AIS counterpart.

Although the LRIT system does not rely on VHF radio signals, as does AIS, the equipment can still be switched off by the shipmaster. Even at the time the MSC adopted the amendments to implement the LRIT system, IMO documents explained that the equipment "shall be capable of being switched off" and cease distribution of the signal when an exceptional circumstance, in the view of the shipmaster, compromises the "safety and security of the ship" (IMO 2006, para. 7). Although it would appear that the security risks associated with unimpeded transmissions of LRIT information are reduced in comparison to AIS, given that LRIT data is only sent to State actors and is generally unavailable to the public (and, therefore, it is not accessible by malign private actors, such as pirates or terrorists), the security switch-off exception reflects the perceived sensitivity of the LRIT vessel-tracking information.

Since its implementation, the AIS framework has been improved by pairing it with newer technologies (Carson-Jackson 2012). In its original form, AIS relied on VHF radio signals that could only be received by equipment carried on vessels or shore-based facilities. This limited its functionality for vessel-tracking purposes. Technical reconfiguration through the use of satellite technology facilitated the collection of AIS signals regardless of whether the transmitting equipment was in relative proximity to the receiving equipment. In the modern era, satellite AIS systems receive, collect, and report vessel identification information, which can then be displayed publicly in highly digestible formats, such as those platforms used by popular ship-tracking websites used by hobbyist ship watchers and shipping industry participants.[18]

As AIS data has been made publicly available through these resources, it has also been incorporated into a range of scientific and economic studies (Armelloni et al. 2021; Dupont et al. 2020; Fournier et al. 2018; Serra-Sogas et al. 2021; Shelmerdine 2018; Svanberg et al. 2019). But AIS has also become an increasingly common source of vessel tracking for use across a range of law enforcement and legal compliance initiatives, often linked to national security concerns (Creech et al. 2003). These uses include repurposing AIS data to track vessels for the purposes of

[18] For instance, marinetraffic.com and vesseltracker.com are popular websites for tracking ships using publicly accessible AIS data.

https://doi.org/10.1017/9781009760171.013 Published online by Cambridge University Press

counteracting piracy, drug trafficking, migrant smuggling, and illegal fishing.[19] Perhaps most of all, regulators have emphasized the use of AIS for the purposes of monitoring economic sanctions compliance at sea (Kilpatrick 2022). At the same time, there is widespread recognition that AIS is not always a reliable source of vessel-tracking data (Goudossis and Katsikas 2019; Harati-Mokhtari et al. 2007). Even satellite AIS is susceptible to technical dropout, given that it fundamentally depends on VHF transmissions. Furthermore, since AIS relies on manual inputs, it can also give rise to unintentional human error. Its dependency on unencrypted VHF channels also makes it vulnerable to external interference, including hacking, jamming, manipulation, and spoofing (Androjna et al. 2021; Wolsing et al. 2022).

Recognizing these vulnerabilities, law enforcement authorities have regularly cited suspicious AIS transmissions – or gaps in AIS signals – as evidence of unlawful activities. At present, one of the most common references to AIS and law enforcement in the compliance context is through an inference of nefarious activity when the vessel operator has switched off the AIS. In this way, rather than simply using AIS to monitor vessels engaging in malfeasance, law enforcement authorities are also analyzing irregularities in AIS signals, which have been referenced to demonstrate malintent. In part to follow regulatory guidance on the subject, commercial actors aiming to monitor the compliance of counterparties or third parties with a nexus to underlying transactions are also carefully monitoring AIS for switch-off or manipulation, which may also be used as an evidentiary source to justify contractual responses.[20]

Further illustrating regulatory interest in AIS gaps, a recent proposal in the US Senate to mobilize new technologies for the purpose of aiding law enforcement officials in tracking vessels, particularly in the sanctions space. For instance, the Vessel Tracking for Sanctions Enforcement Act of 2023 a legislative proposal aimed at requiring US agencies to "assess the feasibility and advisability of using big data analytics to identify and predict instances in which disabling or manipulating [AIS] on a vessel is an indicator that there is a high risk that the vessel is transporting goods in a manner that evades sanctions or export controls."[21]An explanatory document disseminated by the office of one of the Senators who proposed the bill indicates that the program might address the problem of "American law enforcement agencies sifting through huge amounts of data to try to identify bad actors and intervene" (Hassan 2023). As of early 2025, the bill has not moved forward, but it has attracted the attention of the international shipping media (Raanan 2023).

Remarkably, the technologically more reliable LRIT system has been less frequently mentioned in legislative proposals, regulatory guidance, and court documents

[19] Journalistic investigations have also used vessel-tracking technology to demonstrate cargo-laundering activities: see, for example, Diakun (2023a).

[20] Examples of this practice are discussed in Section 7.3.2.

[21] See 118th Congress, 1st Session, S.2248 (2023).

https://doi.org/10.1017/9781009760171.013 Published online by Cambridge University Press

filed by law enforcement authorities seeking to demonstrate vessel involvement in unlawful activities.[22] LRIT data is also rarely deployed as a source of vessel-tracking information in academic studies.[23] The obvious reason for this is that under the LRIT framework, the ship-tracking data is not designed to be made publicly available. Nevertheless, despite these limitations in data distribution, a 2020 Advisory issued by US regulators regarding economic sanctions compliance in the maritime sector cites LRIT data as one factor for shipowners and charterers to consider when engaging in counterparty due diligence (Department of the Treasury et al. 2020, 18). This is an unusual recommendation, as the Advisory fails to acknowledge that LRIT data is not available for scrutiny by private shipping industry participants.

Perhaps in correction, more recent compliance Advisories on the subject either mention only AIS or narrow the LRIT monitoring recommendations to those public actors with access, such as flag States.[24] Emphasizing the role of States in addressing the fallout from vessel-tracking circumvention, a recent IMO Resolution addressing the problem of an expanding "dark fleet" or "shadow fleet" defines the phenomenon as ships that are "engaged in illegal operations" that include "intentionally taking measures to avoid ship detection such as switching off their AIS or LRIT transmissions or concealing the ship's actual identity when there is no legitimate safety or security concern to justify such action" (IMO 2023, para. 1.6).[25] Urging States to combat these practices, since these vessels may have "substandard maintenance, unclear ownership, lack of insurance coverage and disguise their cargoes' destination or origin," the Resolution recommends that port States "subject such ships to enhanced inspections" (IMO 2023, para. 5).

7.3 A NEW ERA IN MARITIME TRANSPARENCY

7.3.1 *Recent Technological Innovations*

In response to the commercial demand created by regulatory mandates and private compliance needs, technology companies have proliferated in efforts to analyze AIS,

[22] Examples of AIS references in law enforcement complaints are discussed in Kilpatrick (2022, 233–238).

[23] At least some academic studies have examined the implications of LRIT data for various purposes. See, for example, Vespe et al. (2015).

[24] See, for example, Price Cap Coalition 2024: "*If accessible, complement AIS Tracking with Long-Range Identification and Tracking ('LRIT')*. In instances of AIS outages or suspected AIS manipulation, stakeholders such as flagging registries that have access to LRIT should use it to determine the true location of vessels, including, where feasible, those leased to third parties. For those industry stakeholders who have access to LRIT, combining AIS and LRIT is a best practice for mitigating risk" (4, emphasis in original).

[25] The Resolution also recalls that "the long-range identification and tracking (LRIT) system can be used to identify ships up to 1,000 nautical miles from the coastal state": IMO (2023, para. 1.6).

https://doi.org/10.1017/9781009760171.013 Published online by Cambridge University Press

LRIT, satellite imagery, and other vessel-tracking data. Described as part of a "transparency revolution" in shipping, the products are building capacity to process varied sources of vessel movement information to make judgments, predictions, and actionable recommendations to flag potentially unlawful behavior (Lloyd's List 2021). These products fall into several categories, including those that repackage AIS in user-friendly platforms, process LRIT or LRIT-analogous data, examine or cross-reference satellite imagery, and compare shipborne transmissions with photographic imagery from shore-based sources.

The market-leading products include those provided by UK-based Lloyd's List Intelligence. In marketing materials, the Lloyd's List program is described as "turning maritime data into actionable insights" (Lloyd's List Intelligence n.d.). This product includes using AI and advanced algorithmic tools to reframe vessel-tracking information collected from a range of sources, including AIS, as a means of assessing risk for legal exposure that can be used for counterparty know-your-customer analysis as required by regulatory mandates (Lloyd's List Intelligence n.d.). Other comparable offerings are provided by Israel-based company Windward, which markets its vessel-screening and fleet-monitoring technology to create predictive commercial intelligence fueled by "Maritime AI" (Windward n.d.). Like the Lloyd's List products, Windward's processes appear to rely on AIS data with operability enhanced through machine-learning analysis with integration into compliance-targeted and user-friendly systems.[26]

Other companies have focused predominantly on satellite imagery analysis. Firms operating in this space include Planet Labs and Maxar Technologies, both of which utilize optical sources to support a variety of surveillance activities, including maritime domain awareness (Maxar n.d.-b; Planet n.d.). Although satellite imagery carries its own limitations, including its high cost and the potential for obstruction by cloudy weather conditions, the variables are diminishing as technology improves. For instance, Maxar has marketed its products as leveraging "synthetic aperture radar" imagery that has the potential to function even in cloud cover (Maxar n.d.-a.).[27] Law enforcement agencies, media outlets, and private sector initiatives have referenced these imagery sources largely as a basis to fact-check AIS switch-off, manipulation, and spoofing. These imagery-based options have the potential to strengthen the credibility of vessel-tracking assessments depending on ship-borne AIS or LRIT data.

Nonsatellite imagery options are also emerging to cross-reference AIS and LRIT. A company called Tanker Trackers, for instance, relies in part on "shoreside photography" to cross-reference other sources of information, including AIS, for sanctions compliance purposes in the oil transport sector (TankerTrackers n.d.). Its findings have been widely shared on social media and through the reporting of

[26] Spire is another company configuring AIS data for compliance-focused tracking: Spire (n.d.).
[27] Other companies are also marketing similar satellite-based options: see ICEYE (n.d.).

https://doi.org/10.1017/9781009760171.013 Published online by Cambridge University Press

major news outlets in investigative journalism on the "dark fleet" (Triebert et al. 2023). Other approaches relying on aerial – and perhaps even undersea – drones may offer similar compliance value as they have the capacity to capture real-time vessel data, particularly as vessels approach geographically narrow areas of navigational significance such as straits and ports (Adamopoulos 2019).[28]

A more controversial option is the commercial marketability of LRIT data. A UK firm called Pole Star is one company that administers LRIT data collection for use by State actors, such as flag States. But Pole Star has allegedly also offered LRIT-equivalent data for commercial compliance purposes (Bockmann 2020).[29] This has sparked contentious discussion within the maritime community because sharing LRIT data for private compliance processes would appear to run counter to the spirit of the IMO regulations that established LRIT for government eyes only. However, it does raise the possibility that the LRIT architecture could be reimagined to provide vessel-tracking information to a broader array of actors. LRIT utilizes equipment already carried on vessels, and it relays location-tracking transmissions automatically at scheduled intervals without any direct human intervention, which offers promise that these tools could be reconfigured potentially to sidestep dependence on the less secure and less reliable AIS. Whether LRIT can mimic the same broader scope of information relayed by AIS is an open technical question. If it is indeed possible to update the LRIT framework with the relatively minor reconfiguration of existing equipment, this could help promote vessel-tracking transparency reform by offering a stable and economically efficient solution that is derivative of the current IMO-mandated regime.

7.3.2 *Commercial Uses*

Motivated by regulatory guidance and the new technologies available on the market, industry organizations have developed contract clauses that seek to address the risks of switching off AIS transponders (BIMCO n.d.). Recent case law provides examples of the ways that commercial actors have relied on vessel-tracking tools and contract clauses to address compliance issues and grounds for termination due to unlawful activities. These cases provide practical endorsements of the vessel-tracking tools that have recently become available and demonstrate how commercial actors may need to rely on them to protect themselves from legal compliance risk.

One example is an arbitration award decided by the New York-based Society of Maritime Arbitrators resolving a charterparty dispute. In *Brujo Finance Company v. Sea Energy Company*, the parties agreed to a contract to perform consecutive voyages carrying gasoline from "Cristobal to Curacao or Aruba, with Charterer

[28] Researchers have even relied on albatross patterns to track fishing vessels that have turned off vessel-tracking transponders to evade detection (Kornei 2020; Weimerkirch et al. 2019).

[29] This controversy is discussed in more detail in Kilpatrick (2022, 242–243).

https://doi.org/10.1017/9781009760171.013 Published online by Cambridge University Press

having the option of discharging the cargo by means of a ship-to-ship transfer."[30] In response to the charterer's request to perform a ship-to-ship (STS) transfer near Aruba, the shipowner sent a message to charter indicating concern that the STS transfer might involve sanctioned Venezuelan cargo. The message read: "Owners WILL NOT participate in any illegal trading. If the intention is to transship the cargo [STS] to move it to Venezuela same will not be done. Any vessel nominated for transshipment will be subject to strict anti-sanctions scrutiny." Then, the charterer informed the shipowner that the proposed STS transfer would involve a vessel called the MT *Beauty One*. In an attempt to assure the shipowner that the vessel would not be engaged in any kind of sanctions-busting trades, the charterer emphasized to the shipowner that the *Beauty One* was not on any US sanctions lists.

After being notified that the proposed STS transfer would involve the *Beauty One*, the shipowner obtained documents from an external "tracking service" indicating that the vessel had made several calls to Venezuelan ports during the previous year. On that basis, the shipowner noted that all parties involved in the transaction could become sanctioned by US authorities if the transaction involved a Venezuelan nexus. The shipowner then referenced the *Beauty One*'s "recent trading history exclusively in Venezuelan waters" as a basis to seek additional assurances of legal compliance. But the charterer did not provide additional assurances meeting the shipowner's standards, so the shipowner wrote back to the charterer explaining that "saying 'trust us'" is insufficient to provide assurances of compliance. The shipowner then invoked a sanctions clause in the charterparty on grounds that the charterers had failed to give assurances that the *Beauty One* would not perform an unlawful trade.

In the arbitration proceedings that followed, the Society of Maritime Arbitrators held in favor of the shipowner. The arbitral panel reasoned that there was sufficient evidence to determine that there was a "discernible risk" that facilitating the transaction with the *Beauty One* could trigger US sanctions. As evidence of this risk, the panel referenced the reported trading history of the *Beauty One* as a relevant consideration. Since the charterer did not provide any contrary evidence of the *Beauty One*'s previous trading history, this caused the panel to find that the shipowner properly invoked the sanctions clause by refusing the charterer's orders to engage in an STS transaction that "could expose" it to US sanctions.

Another recent case involving reference to vessel tracking is *Kuvera Resources Pte Ltd v. JPMorgan Chase Bank NA*, which was decided by the Court of Appeal of the Republic of Singapore (Kilpatrick 2023).[31] In that case, a Singaporean trading company was the beneficiary of letters of credit linked to transactions of coal that

[30] *Brujo Finance Company v. Sea Energy Company*, SMA 4388 (July 3, 2020). The quotations that follow are from this decision.

[31] *Kuvera Resources Pte Ltd v. JPMorgan Chase Bank NA* [2023] SGCA 28. The quotations that follow are from this decision.

https://doi.org/10.1017/9781009760171.013 Published online by Cambridge University Press

had been moved from Indonesia to the Middle East. In attempts to collect under the letters of credit, the trading company went to the Singapore branch of US bank JPMorgan Chase and presented documents compliant with the letters of credit. When the bank performed its internal compliance check, it determined that a vessel that had moved coal in the underlying trade had previously used another name and had been beneficially owned by a Syrian national, which made it potentially subject to US sanctions. On that basis, the bank refused to pay on the letters of credit and invoked the sanctions clause that granted it the liberty to avoid payment if documents presented involved a "vessel" subject to sanctions.

The trial court held in favor of the bank on grounds that since the vessel was apparently previously owned by an actor subject to US sanctions, the name and registration change would have been viewed as an attempt to mask its true identity, which could expose the bank to sanctions if it paid on the letters of credit. The Court of Appeal reversed that decision, however, in part because it determined that the sanctions clauses in the letters of credit contained an implicit burden of proof that the bank did not meet. That burden of proof required the bank to demonstrate that the vessel was "Syrian-owned at all material times." It reasoned that due in part to commercially available vessel-tracking information, this was a fact that was "capable of objective determination." As evidence of this, the court referenced the Lloyd's List Intelligence database (discussed above), which apparently showed that during the relevant period, the vessel owner and various operating entities did not have a direct Syrian nexus.

7.3.3 *Security Risks*

The paradoxical challenge of promoting vessel location transparency while also maintaining maritime security has come into focus during the recent emergence of security threats for vessels moving through the Red Sea. Citing the deteriorating humanitarian conditions associated with the Israel–Hamas War and utilizing weapons apparently provided by Iran, Houthi militias occupying substantial territory in Yemen have attacked dozens of merchant ships in and around the Red Sea. These events have been so disruptive that they caused many ships to reroute around the Cape of Good Hope rather than risk transit through the Suez Canal. They also led to condemnations by a UN Security Council Resolution and coalition airstrikes inside Yemeni territory (UNSC 2024a).

Although these Houthi attacks have impacted vessels with a nexus to a broad range of national interests, according to statements made by Houthi leaders, there has been at least some attempt to target vessels with links to "enemy" States (Bockmann 2024b). The Houthis initially claimed to target vessels with an Israeli connection. But determining the Israeli nexus of merchant ships is a complicated endeavor that might involve layers of connections, including the vessel's flag, place of beneficial ownership, place of management, and ports of origin and discharge, as

https://doi.org/10.1017/9781009760171.013 Published online by Cambridge University Press

well as the trading history, the cargo carried on board, the place of the vessel's various insurers, and, of course, the nationalities of the seafarers on board. As an illustration of this complexity, ships operated by the Swiss-based Mediterranean Shipping Company have been targeted more than other container lines, apparently because one of the company's shareholders holds an Israeli passport (as well as Swiss and Italian passports); (Lloyd's List 2024).

In response to this threat, vessel operators in the region begin utilizing their vessel-tracking transponders to send messages to the Houthis indicating their lack of any Israeli connection and to indicate the presence of armed guards on board. According to media outlets, vessel operators have used their AIS signals to relay messages such as "NOLINKISRAEL," "ALL CHINESE CREW," "ALLRUSSIAN," and "RUSSIA+CHINA" (Maritime Executive 2023). Houthi leaders have even issued statements on social media addressed to "ministries of transport in all countries of the world and to international shipping companies," requesting vessel operators to utilize their vessel-tracking transponders to relay such information – including "no relationship to Israel" (Raanan 2024).

In attempts to ascertain these various factors, it appears that Houthis have been engaged in some level of investigation when determining whether to attack a given vessel. This is thought to have involved utilizing commercial vessel-tracking products, as well as more sophisticated intelligence gathering from State allies such as Iran (Bryen 2023; Faucon et al. 2023). But, despite attempts by vessel operators to communicate regarding any potential political risk associated with a vessel, and despite the Houthi "investigations" into vessel affiliations, the attacks on vessels with apparently neutral connections demonstrate the arbitrary nature of the Houthi strategy.

In part due to this risk, regulators have issued guidance indicating that vessels operating in the Red Sea should deactivate their vessel-tracking transponders to complicate the Houthis' ability to locate them. For instance, the US Maritime Administration issued an Advisory in March 2024 regarding threats to commercial vessels (MARAD 2024). It advises that "U.S.-flagged vessels transiting the Southern Red Sea, Bab el Mandeb Strait, and Gulf of Aden with AIS transponders on are at increased risk of targeting by adversarial actors" (MARAD 2024). Accordingly, the Advisory relays the position that vessel operators are "strongly advised to turn off their AIS transponders unless vessel Masters believe that doing so would compromise the safety of the vessel" (MARAD 2024). The Advisory explains that "while vessels have been attacked by the Houthis while transponders were on and while off, turning AIS off makes it more difficult to track and accurately target a vessel" (MARAD 2024). It then notes that "adherence to all flag state and international requirements and guidance regarding operation of AIS, and the safe navigation of the vessel, remains the responsibility of individual companies and vessel Masters" (MARAD 2024).[32]

[32] A sanctions compliance Advisory issued by the US regulators in September 2024 highlights this challenge of balancing transparency and risk: "There can be legitimate reasons for AIS to be

https://doi.org/10.1017/9781009760171.013 Published online by Cambridge University Press

Simultaneously, UK authorities have made different recommendations on the basis that Houthis have attacked both vessels with AIS switched off and vessels with AIS switched on, indicating that they may have other means of tracking vessels. A February 2024 Advisory issued by UK Maritime Trade Operations (UKMTO) explains that "turning off AIS makes it marginally more difficult to track a ship but may also hinder the ability of the military to provide support or direct contact" (UKMTO 2024). The Advisory notes: "Limiting the information in AIS data fields or switching off AIS could make a ship harder to locate, but it is unlikely to prevent an attack. Limiting AIS data to the mandatory fields and omitting the next port of call (NPOC) could be considered" (UKMTO 2024).

Insurers, being critical stakeholders as they may be responsible for paying claims in the event of an attack, have also weighed in on what shipmasters should do to avoid risk in the Red Sea. Although war risk insurers have not publicly issued guidance indicating whether vessel operators should keep AIS switched off or on, protection and indemnity clubs have issued circulars on the matter. Swedish insurer Skuld, for instance, has explained that "some ships have been targeted despite having their AIS turned off, suggesting that the Houthis have alternative methods of identifying and tracking their targets" (Skuld 2024).

These regulatory and commercial best practices advocating for vessel operators to deactivate vessel-tracking transponders are a stark juxtaposition to the vessel transparency mandates provided by regulators and commercial actors reacting to other compliance concerns, especially in the sanctions context. Vessel operators are compelled through both regulation and contractual obligations to evaluate carefully the circumstances in which the vessel-tracking transponders should remain on or be switched off. These distinct risks demonstrate that such decisions cannot be made relying on a bare reading of SOLAS or the IMO Guidelines but instead require vessel operators to use holistic judgment depending on a range of legal compliance and security factors.

7.4 CONCLUSION

As vessel tracking is adopted for law enforcement and compliance initiatives, the technological standards for consistent and accurate monitoring capacity are growing exponentially. Although vessel-tracking tools have rapidly expanded in recent years, they still largely rely on voluntary shipborne transmissions the user or third-party interference can manipulate. Efforts to enhance vessel tracking beyond the status

turned off or 'go dark' (e.g., passage through waters at high-risk of piracy or due to other security considerations). In such situations, it is advisable for ships to turn off their AIS to evade threats, and thus should not be considered a red flag for illicit activity. However, ship registries, insurers, charterers, vessel owners, or port operators should consider investigating vessels that appear to have turned off their AIS transponders for extended periods or unknown reasons while operating in the Mediterranean and Red Seas" (OFAC 2024).

https://doi.org/10.1017/9781009760171.013 Published online by Cambridge University Press

quo will require the implementation of new tools and techniques that rectify the vulnerabilities of current processes. These advances in machine learning, AI, satellite imagery, and aerial and undersea drones, along with other operational improvements, will undoubtedly facilitate the regulatory demand for maritime transparency. The success of these new models will be driven by the ingenuity of engineers and code-writers rather than policy analysts, but as capacity quickly builds, it may only be a matter of time before monitoring tools are able to track vessels without reliance on shipborne equipment at all. In reimagining a vessel-tracking standard, these new tools will create highly valuable insights that may facilitate the regulation of the "dark fleet" and its shadowy activities. But, as recent events tragically demonstrate, this unprecedented visibility may beget pronounced security risks.

REFERENCES

Adamopoulos, Anastassios. 2019. "Denmark Turns to Drones for Sulphur Compliance." *Lloyd's List*, April 15.

Androjna, Andrej, Marko Perkovič, Ivica Pavic, and Jakša Miškovič. 2021. "AIS Data Vulnerability Indicated by a Spoofing Case-Study." *Applied Sciences* 11 (11): 5015.

Armelloni, Enrico Nicola, Anna Nora Tassetti, Carmen Ferrà, Alessandro Galdelli, Martina Scanu, Adriano Mancini, Gianna Fabi, and Giuseppe Scarcella. 2021. "AIS Data, a Mine of Information on Trawling Fleet Mobility in the Mediterranean Sea." *Marine Policy* 129: 104571.

Baker, W. J. 1971. *A History of the Marconi Company*. St. Martin's Press.

BIMCO (Baltic and International Maritime Council). n.d. "AIS Switch Off Clause 2021." www.bimco.org/contracts-and-clauses/bimco-clauses/current/ais_switch_off_clause_2021.

Bockmann, Michelle Wiese. 2020. "Government-Only Vessel-Tracking Data Up for Sale 'with US Approval.'" *Lloyd's List*, June 19.

2024a. "Dark Fleet Tanker Reportedly Detained off Finland after Undersea Cable Cut." *Lloyd's List*, 26 December.

2024b. "Greece-Owned Ships Are Top Houthi Target." *Lloyd's List*, October 23.

Bréhaut, Denise. 2013. *GMDSS: A User's Handbook*. 5th ed. Bloomsbury.

Bryen, Stephen. 2023. "Iran-Houthis Tap AIS Tracking Tech for High Seas Attacks." *Asia Times*, December 25.

Carson-Jackson, J. 2012. "Satellite AIS: Developing Technology or Existing Capability?" *Journal of Navigation* 65 (2): 303–321.

Creech, Jay A., and Joseph F. Ryan. 2003. "AIS, The Cornerstone of National Security?" *Journal of Navigation* 56 (1): 31–44.

Diakun, Bridget. 2023a. "Shadowy Trade in 'Stolen' Grain from Russia-Occupied Azov Ramps Up." *Lloyd's List*, 8 September.

2023b. "US-Sanctioned Crimea Caller and Accused Grain Plunderer Renames." *Lloyd's List*, November 2.

Department of the Treasury, Department of State, and Coast Guard (United States). 2020. "Sanctions Advisory for the Maritime Industry, Energy and Metals Sectors, and Related Communities." May 14.

Dupont, Clement, Françoise Gourmelon, Catherine Meur-Ferec, Frédérick Herpers, and Christophe Le Visage. 2020. "Exploring Uses of Maritime Surveillance Data for Marine Spatial Planning: A Review of Scientific Literature." *Marine Policy* 117: 103930.

https://doi.org/10.1017/9781009760171.013 Published online by Cambridge University Press

Faucon, Benoit, Dov Lieber, and Gordon Lubold. 2023. "Iranian Spy Ship Helps Houthis Direct Attacks on Red Sea Vessels." *Wall Street Journal*, December 22.
Fournier, Melanie, R. Casey Hilliard, Sara Rezaee, and Ronald Pelot. 2018. "Past, Present, and Future of the Satellite-Based Automatic Identification System: Areas of Applications (2004–2016)." *WMU Journal of Marine Affairs* 17: 311–345.
Goudossis, Athanassios, and Sokratis K Katsikas. 2019. "Towards a Secure Automatic Identification System (AIS)." *Journal of Marine Science and Technology* 24 (6): 410–423.
Harati-Mokhtari, Abbas, Alan Wall, Philip Brooks, and Jin Wang. 2007. "Automatic Identification Systems (AIS): Data Reliability and Human Error Implications." *Journal of Navigation* 60 (3): 373–389.
Hassan, Maggie. 2023. "Vessel Tracking for Sanctions Enforcement Act of 2023." www.dco.uscg.mil/Portals/9/DCO%20Documents/Proceedings%20Magazine/Archive/2012/Vol69_No2_Sum2012.pdf
Hersey, Joe. 2012. "Radio Communications from the Time of the Titanic." Proceedings (US Coast Guard), Summer. www.dco.uscg.mil/Portals/9/DCO%20Documents/Proceedings%20Magazine/Archive/2012/Vol69_No2_Sum2012.pdf.
ICEYE. n.d. "Maritime Domain Awareness." www.iceye.com/sar-data/use-cases/maritime-domain-awareness.
IMO (International Maritime Organization). 2000a. "Guidelines on Automatic Identification of Shipping (AIS) Operational Matters: Note by the International Chamber of Shipping (ICS)." MSC 72/10/12 (May 31, 2000).
2000b. "Adoption of Amendments to the International Convention for the Safety of Life at Sea, 1974, as Amended." MSC.99(73) (December 5, 2000).
2000c. "Revision of Chapter V of SOLAS: Transponders." Submitted by INTERTANKO. MSC 72/10/8 (March 14, 2000).
2001. "Guidelines for the Onboard Operational Use of Shipborne Automatic Identification Systems (AIS)." A 22/Res.917 (November 29, 2001).
2006. "Adoption of Amendments to the International Convention for the Safety of Life at Sea, 1974, as Amended." MSC.202(81) (May 19, 2006).
2012. *Guide to Maritime Security and the ISPS Code*.
2015. "Revised Guidelines for the Onboard Operational Use of Shipborne Automatic Identification Systems (AIS)." A 29/Res.1106 (December 14, 2015), Annex.
2023. "Urging Member States and All Relevant Stakeholders to Promote Actions to Prevent Illegal Operations in the Maritime Sector by the 'Dark Fleet' or 'Shadow Fleet.'" A 33/Res.1192 (December 11, 2023).
n.d. "Brief History of IMO." www.imo.org/en/About/HistoryOfIMO/Pages/Default.aspx.
Kilpatrick, Richard L., Jr., 2022. "Monitoring Sanctions Compliance at Sea." *Northwestern Journal of International Law and Business* 42 (2): 221–251.
2023. "Sanctions Clause Redux." *Journal of International Maritime Law* 29 (4): 199.
Kornei, Katherine. 2020. "They're Stealthy at Sea, but They Can't Hide from the Albatross." *New York Times*, January 29.
Krajewski, Jason M. 2008. "Out of Sight, Out of Mind? A Case for Long Range Identification and Tracking of Vessels on the High Seas." *Naval Law Review* 56: 219–249.
Lloyd's List. 2021. *Transparency in Shipping: A Special Report*. Informa.
2024. "Ships Should Not Be Attacked on the Basis of an Owner's Passport." *Lloyd's List*, May 10.
2025. "UK-Led Alliance Using AI to Monitor Threats to Undersea Cables." *Lloyd's List*, January 7.
Lloyd's List Intelligence. n.d. "About Us: Our Data." www.lloydslistintelligence.com/about-us/our-data.

https://doi.org/10.1017/9781009760171.013 Published online by Cambridge University Press

MARAD (United States Maritime Administration). 2024. MSCI Advisory 2024-004: Southern Red Sea, Bab el Mandeb Strait, Gulf of Aden, Indian Ocean, Somali Basin, Arabian Sea, Gulf of Oman, Strait of Hormuz, and Persian Gulf – Threats to Commercial Vessels.
Maritime Executive. 2023. "Report: Ships Make Novel Use of AIS to Ward Off Attacks by Houthis." *Maritime Executive*, December 28.
Mathews, Sean. 2024. "How the Houthis Mined Commercial Intelligence to Sabotage Global Trade." *Middle East Eye*, September 5. www.middleeasteye.net/news/how-houthis-mined-commercial-intelligence-sabotage-global-trade.
Maxar. n.d.-a. "Crow's Nest." www.maxar.com/maxar-intelligence/products/crows-nest.
n.d.-b. "Near Real-Time Vessel Detection." https://explore.maxar.com/maritime-monitoring.html.
NATO (North Atlantic Treaty Organization). 2021. "AIS (Automatic Identification System) Overview." https://shipping.nato.int/nsc/operations/news/2021/ais-automatic-identification-system-overview.
New York Times. 1912. "Titanic Sinks Four Hours after Hitting Iceberg; 866 Rescued by Carpathia, Probably 1250 Perish; Ismay Safe, Mrs. Astor Maybe, Noted Names Missing." *New York Times*, April 15.
OFAC (United States Department of the Treasury, Office of Foreign Assets Control). 2024. "OFAC Advisory to the Maritime Petroleum Shipping Community: Sanctions Risks Related to Petroleum Shipments Involving Iran and Syria." September 11.
Photo Museum Ireland. n.d. "The Marconi Room, on Board the Titanic." https://timeline.photomuseumireland.ie/timeline/the-marconi-room-on-board-the-titanic/.
Planet. n.d. "Maritime and Coastal Monitoring from Planet." www.planet.com/industries/maritime/.
Price Cap Coalition. 2024. "Updated Price Cap Coalition Advisory for the Maritime Oil Industry and Related Sectors: Best Practices in Response to Recent Developments in the Maritime Oil Trade." October 21.
Raanan, Tomer. 2023. "US Lawmakers Mulling AIS-Spoofing Bill as Iran's Oil Export Surge." *Lloyd's List*, 31 August.
2024. "Houthi Leader Tells Ships to Deny Israel Links on AIS." *Lloyd's List*, January 8.
Serra-Sogas, Norma, Patrick D. O'Hara, Kim Pearce, Leh Smallshaw, and Rosaline Canessa. 2021. "Using Aerial Surveys to Fill Gaps in AIS Vessel Traffic Data to Inform Threat Assessments, Vessel Management, and Planning." *Marine Policy* 133: 104765.
Shelmerdine, Richard L. 2018. "Teasing Out the Detail: How Our Understanding of Marine AIS Data Can Better Inform Industries, Developments, and Planning." *Marine Policy* 54: 17–25.
Skuld. 2024. "Updated Threats to Shipping in the Red Sea." www.skuld.com/topics/port/piracy/updated-threats-to-shipping-in-the-red-sea/.
Spire. n.d. "Maritime AIS Data for Vessel Tracking." https://spire.com/maritime/.
Svanberg, Martin, Vendela Santén, Axel Hörteborn, Henrik Holm, and Christian Finnsgård. 2019. "AIS in Maritime Research." *Marine Policy* 106: 103520.
Sweeney, Michael. 2024. "'Darking' AIS: US and UK Maritime Agencies Split on Strategy to Protect Vessels in Red Sea." *Intelligence Online*, May 20. www.intelligenceonline.com/government-intelligence/2024/05/20/-darking–ais-us-and-uk-maritime-agencies-split-on-strategy-to-protect-vessels-in-red-sea,110227492-art.
TankerTrackers. n.d. "Tracking for a Transparent Oil Market." https://tankertrackers.com.
Triebert, Christiaan, Blacki Migliozzi, Alexander Cardia, Muyi Xiao, and David Botti. 2023. "Fake Signals and American Insurance: How a Dark Fleet Moves Russian Oil." *New York Times*, May 30.

https://doi.org/10.1017/9781009760171.013 Published online by Cambridge University Press

UKMTO (United Kingdom Maritime Trade Operations). 2024. "Notice, Interim Industry Transit Advice, Southern Red Sea and Gulf of Aden." February 5.

UNSC (United Nations Security Council). 2024a. Resolution 2722. S/RES/2722 (January 10, 2024).

2024b. Resolution 2739. S/RES/2739 (June 27, 2024).

USCG (United States Coast Guard). n.d. "Global Maritime Distress and Safety System." Navigation Center. www.navcen.uscg.gov/global-maritime-distress-and-safety-system.

Vespe, Michele, Harm Greidanus, and Marlene Alvarez Alvarez. 2015. "The Declining Impact of Piracy on Maritime Transport in the Indian Ocean: Statistical Analysis of 5-Year Vessel Tracking Data." *Marine Policy* 59: 9–15.

Weimerkirch, Henri, Julien Collet, Alexandre Corbeau, Adrien Pajot, Floran Hoarau, Cédric Marteau, Dominique Filippi, and Samantha C. Patrick. 2019. "Ocean Sentinel Albatrosses Locate Illegal Vessels and Provide the First Estimate of the Extent of Nondeclared Fishing." *PNAS* 117 (6): 3006–3014.

Windward. n.d. "About Us." https://windward.ai/company/about-us/.

Wolsing, Konrad, Linus Roepert, Jan Bauer, and Klaus Wehrle. 2022. "Anomaly Detection in Maritime AIS Tracks: A Review of Recent Approaches." *Journal of Marine Science and Engineering* 10 (1): 112.

https://doi.org/10.1017/9781009760171.013 Published online by Cambridge University Press

https://doi.org/10.1017/9781009760171.013 Published online by Cambridge University Press