

UNMASKED

VESSEL IDENTITY LAUNDERING AND
NORTH KOREA'S MARITIME SANCTIONS EVASION



ABOUT C4ADS

C4ADS (www.c4ads.org) is a 501(c)(3) nonprofit organization dedicated to data-driven analysis and evidence-based reporting of conflict and security issues worldwide. Our approach leverages nontraditional investigative techniques and emerging analytical technologies. We recognize the value of working on the ground in the field, capturing local knowledge, and collecting original data to inform our analysis. At the same time, we employ cutting edge technology to manage and analyze that data. The result is an innovative analytical approach to conflict prevention and mitigation.

© C4ADS 2021

ABOUT THE AUTHORS

Andrew Boling is a Research Consultant for the Counterproliferation Cell at C4ADS, where he analyzes North Korea-related maritime activity and Chinese technology strategy. He holds a B.S. in International Politics from Georgetown University and speaks Mandarin Chinese.

Lucas Kuo is a Senior Analyst on the Counterproliferation Cell at C4ADS, where he focuses on North Korean illicit shipping, financial, and procurement networks and their connections to organized crime. Prior to joining C4ADS, Lucas' experience spanned the Congressional Executive Commission on China and U.S. Department of State. He holds a B.A. in International Affairs from the George Washington University, and speaks Mandarin Chinese.

Luke Snyder is a Research Consultant for the Counterproliferation Cell at C4ADS, where he analyzes North Korea-related maritime activity and associated sanctions-evasion networks. He holds a B.S. in Regional and Comparative Studies from Georgetown University and speaks Mandarin Chinese.

Lauren Sung is an Analyst on the Counterproliferation Cell at C4ADS. She specializes in East Asia research, focusing on North Korea's proliferation financing, Chinese overseas investment, and transnational organized crime. Prior to C4ADS, Lauren worked in strategic advisory consulting and political risk. She received her M.A. in Asian Studies at Georgetown University's School of Foreign Service and her B.A. from the University of Cambridge.

ACKNOWLEDGEMENTS

C4ADS would like to thank all those who provided input and guidance throughout the course of this research project. The authors are particularly grateful to IHS Markit for sharing subject matter expertise and providing investigative support. The authors also thank the Data Cell at C4ADS, whose data collection and software development efforts were critical to this issue brief's findings, peer reviewers who provided feedback on writing, and Anna Wheeler and Lilli Mercho for providing design and communications support.

C4ADS gives special thanks to our technology partners, whose data, software, and assistance were integral to breakthroughs in research and analysis.

ANALYSIS POWERED BY



WINDWARD[®]



IHS Markit[™]



AIRBUS

MAXAR

Cover image adapted from a photograph taken by NK News, used with permission.

LEGAL DISCLAIMER

The mention of any individual, company, organization, or other entity in this report does not imply the violation of any law or international agreement, and should not be construed to so imply.

GLOSSARY

Automatic Identification System (AIS) Transponder: An AIS transponder is a ship-mounted device that uses radio and GPS technology to provide information about the vessel, such as identity, position, course, and speed, to surrounding vessels as well as land- and satellite-based receivers. In 2000, the International Maritime Organization adopted a requirement for all ships at or above 300 gross tonnage and engaged on international voyages to be equipped with an AIS transponder, effective December 2004.¹

“Clean” Vessel: A vessel that has not been the subject of derogatory reporting or law enforcement action that would inhibit its ability to engage in normal commercial activity. So-called “dirty” vessels may masquerade as clean vessels in order to conduct activities that would be prohibited or difficult under their own identities.

Dark Voyage: A voyage or portion of a voyage made by a ship during a period of no AIS transmission.

Deadweight Tonnage: The weight in metric tons (1000 kg) of cargo, stores, fuel, passengers, and crew carried by the ship when loaded to the vessel's maximum draft.²

DPRK: The Democratic People's Republic of Korea, also known as North Korea. The terms will be used interchangeably in this issue brief.

Designation / Sanctioning: A disciplinary status applied to an entity by a regulatory body. For the purposes of this report, designation will refer to sanctioning by the United Nations Security Council's 1718 Committee, charged with drafting, implementing, and reporting North Korea-related sanctions.³

Digital Identity: The static, dynamic, and voyage-related information transmitted by the vessel's AIS transponder.

“Dirty” Vessel: A vessel subject to public derogatory reporting or law enforcement action that may inhibit its ability to engage in commercial operations at will.

Cover/Disguise Identity: Any physical, digital, or registered identity fraudulently adopted by a vessel to obfuscate its true identity.

Fabricated Identity: An identity assumed by a vessel which corresponds to a fraudulently obtained, registered IMO number.

Flag State: The country for the registry under which the vessel operates. Vessels may appear in more than one registry (parallel registry), although only one of them may be active at a time.⁴

Global Integrated Shipping Information System (GISIS): An informational data hub developed, operated, and maintained by the IMO to assist global shipping industry and maritime professionals in complying with different types of rules and regulations, global and local.⁵

Intermediary Vessel: A clean vessel that vacates its identity for a dirty vessel to assume.

International Maritime Organization (IMO): The United Nations' specialized agency responsible for developing and preserving a comprehensive framework of regulations and policies for the shipping industry and its activities, such as issues of maritime security, safety, technical cooperation, and environmental concerns, as well as legal matters.^{6 7}

IMO Number: A unique seven-digit number which remains unchanged during the life of the ship and remains constant in the event of rebuilding or ship type conversion. This unique number is assigned to the total or greater portion of the hull enclosing the machinery space and is the determining factor should additional hull sections be added. The IMO Number is never reassigned to another vessel.⁸

Maritime Mobile Service Identity (MMSI): Nine-digit number used by AIS and certain other radio equipment to uniquely identify a ship or a coast radio station.⁹

Physical Identity: A vessel's physical identity is determined by its observable features which can include cosmetic (e.g. paint scheme), structural (e.g. hull design, deck configuration, pipelines, engine, etc.) and measured (e.g. length and breadth) characteristics.

Registered Identity: The suite of information linked to a vessel's IMO number. As the international regulator of maritime and shipping affairs, the IMO ship registration and number system is considered authoritative.

Shell Identity: An identity assumed by a vessel which corresponds to a fraudulently obtained, registered IMO number.

Ship-to-Ship (STS) Transfer: The transfer of cargo between two vessels positioned alongside each other.¹⁰

SOLAS: The International Convention for the Safety of Life at Sea (SOLAS), an international maritime treaty which sets minimum safety standards in the construction, equipment and operation of merchant ships.¹¹

UN Panel of Experts Established Pursuant to Resolution 1874 (2009): A group of up to eight experts gathering, examining, and analyzing evidence from United Nations Member States to assist and make recommendations supporting the Security Council Committee established pursuant to Resolution 1718.¹²

United Nations Security Council (UNSC): Responsible for the maintenance of international peace and security, the UNSC is tasked with the power to enact sanctions and issue binding resolutions on all Member States.

Vacated Identity: A digital identity that is no longer being transmitted by its registered user, thereby leaving it open to being assumed by a secondary vessel intending to masquerade as the vessel whose digital identity has been vacated.

Vessel Identity Laundering: An operation in which one or more ships deliberately tampers with or misrepresents aspects of its physical, digital, and registered identities to obfuscate its original identity and necessitates at least one ship assuming a fraudulently obtained, IMO-registered “shell” identity. In a Type 1, or “direct” laundering operation, the dirty vessel directly assumes the shell identity. In a Type 2, or “indirect” operation, a clean vessel assumes the shell identity and the dirty vessel assumes the clean vessel's now-vacant identity.

Vessel Identity Tampering: The deliberate falsification of a vessel's broadcasted data on AIS and/or alterations to its physical features to misrepresent its identity.

EXECUTIVE SUMMARY

Vessel identity laundering operations jeopardize the integrity of the International Maritime Organization (IMO) ship registration system, which the world relies upon in order to identify, track, and interact with the 60,000 ships that travel the world's oceans transporting 90% of global trade.

Vessel identity laundering is a novel tactic in which one or more vessels adopt a different identity on Automatic Identification System (AIS) transmissions in order to allow “dirty” (i.e. associated with illicit activities) ships to assume “clean” identities, and involves at least one vessel in this operation assuming an identity that is obtained by defrauding the IMO. Vessel identity laundering is significantly more sophisticated than previously observed instances of “vessel identity tampering,” in which vessels modify their physical appearance or broadcast false data on AIS transmissions. Given its complexity, vessel identity laundering presents unprecedented challenges for maritime regulators and risks undermining global shipping practices.

In recent years, C4ADS has observed at least 11 ships engaging in elaborate schemes to create fraudulent ship registrations with the IMO, which are subsequently used to “launder” the identity of vessels that have been associated with illicit activities. In particular, we have seen networks involved in DPRK sanctions evasion and smuggling use these tactics to avoid the heightened scrutiny of the sanctions regime.

This issue brief seeks to empower law enforcement and civil regulators to detect and disrupt vessel identity laundering operations by explaining how vessel identity laundering operations work and demonstrating how they can be detected using AIS data, satellite imagery, IMO registration records, and other sources of publicly available information. We cover two previously unreported case studies of vessel identity laundering involving DPRK fuel smuggling networks:

- The KINGSWAY (IMO 9191773), sanctioned by the UN Security Council (UNSC) for engaging in a ship-to-ship transfer with a North Korean tanker, laundered its identity into the APEX/SHUN FA (IMO 8528864) in late 2018.
- The SUBBLIC (IMO 8126082), recommended for designation by the UN Panel of Experts for numerous deliveries of fuel to North Korea, laundered its identity into the HAI ZHOU 168 (IMO 8514045) in mid-2019.

This report finds that in order to counter vessel identity laundering, the IMO and other maritime regulators must take steps to strengthen due diligence processes to secure a ship's registered, digital, and physical identities. We offer recommendations to prevent the proliferation of fraudulent ship identities and mitigate risk by improving data collection, authentication, and transparency.

TABLE OF CONTENTS

GLOSSARY4

EXECUTIVE SUMMARY7

TABLE OF CONTENTS8

WHAT CONSTITUTES A SHIP'S IDENTITY?9

VESSEL IDENTITY LAUNDERING: TWO TYPOLOGIES17

TYPE 1 DIRECT VESSEL IDENTITY LAUNDERING: THE KINGSWAY27

TYPE 2 INDIRECT VESSEL IDENTITY LAUNDERING: THE SUBBLIC36

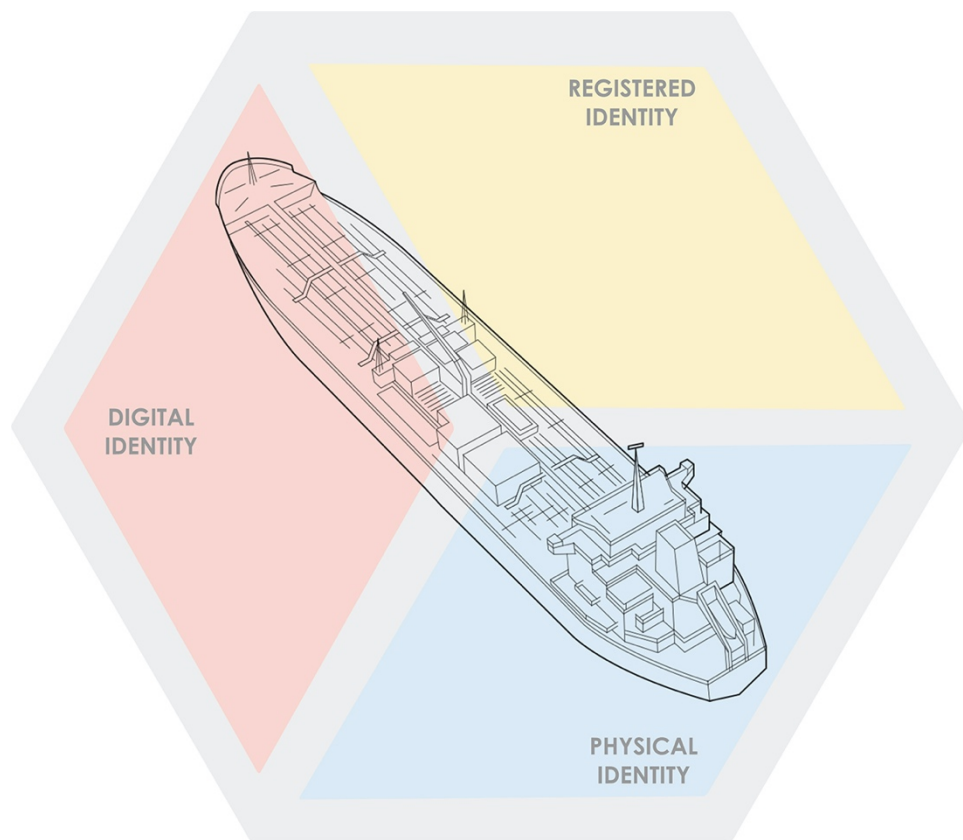
KEY TAKEAWAYS44

RECOMMENDATIONS50

END NOTES54

WHAT CONSTITUTES A SHIP'S IDENTITY?

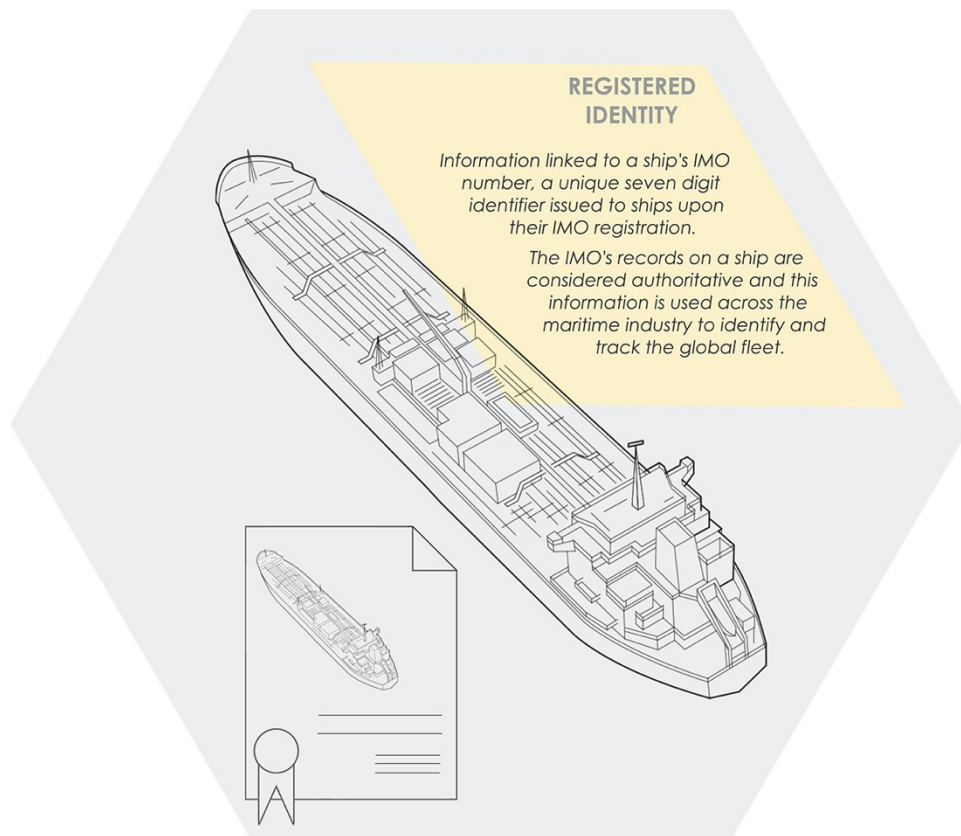
A ship's identity consists of three core facets: registered, digital, and physical. These three groups of information are used both separately and in tandem to identify ships at sea. Each serves an important purpose: a ship's registered identity functions as a credible record of a ship's existence and features; its digital identity is used in the remote tracking of a ship's movements; and a ship's physical identity provides visual evidence of a ship's identifying information and purpose.



The accurate assessment of a ship's identity is critical for reasons ranging from facilitating the efficient flow of global commerce to ensuring maritime safety and security. For instance, ships at sea need ways to verify that their counterpart in a ship-to-ship interaction is indeed who they say they are. Financial institutions need documents to establish a ship's identity and assess its condition to underwrite loans. Government and law enforcement agencies, such as a nation's coast guard, need to identify ships across a state's territorial waters to enforce maritime regulations. Port authorities, who oversee heavy vessel traffic within narrow waterways, must be able to identify ships in order to track their movements and communicate with them effectively.

Illicit actors, on the other hand, want to remain unidentified, and try to obfuscate their ship's activities and their relationships with it. They employ a variety of methods to tamper with their ship's identity or to otherwise misrepresent their activities, resulting in a continuous game of cat and mouse between maritime enforcers and those seeking to escape regulation.

REGISTERED IDENTITY



A vessel's registered identity is the set of information linked to its IMO number, a unique seven-digit number assigned by IHS Markit on behalf of the IMO upon registration. As the international regulator of maritime and shipping affairs, the IMO ship registration and number system is considered authoritative, and this information is used across the maritime industry to identify and track ships in the global fleet. A vessel's registration with the IMO confers a level of legitimacy that enables the vessel to access the regulatory and financial services it needs to operate safely and engage in commercial activity.

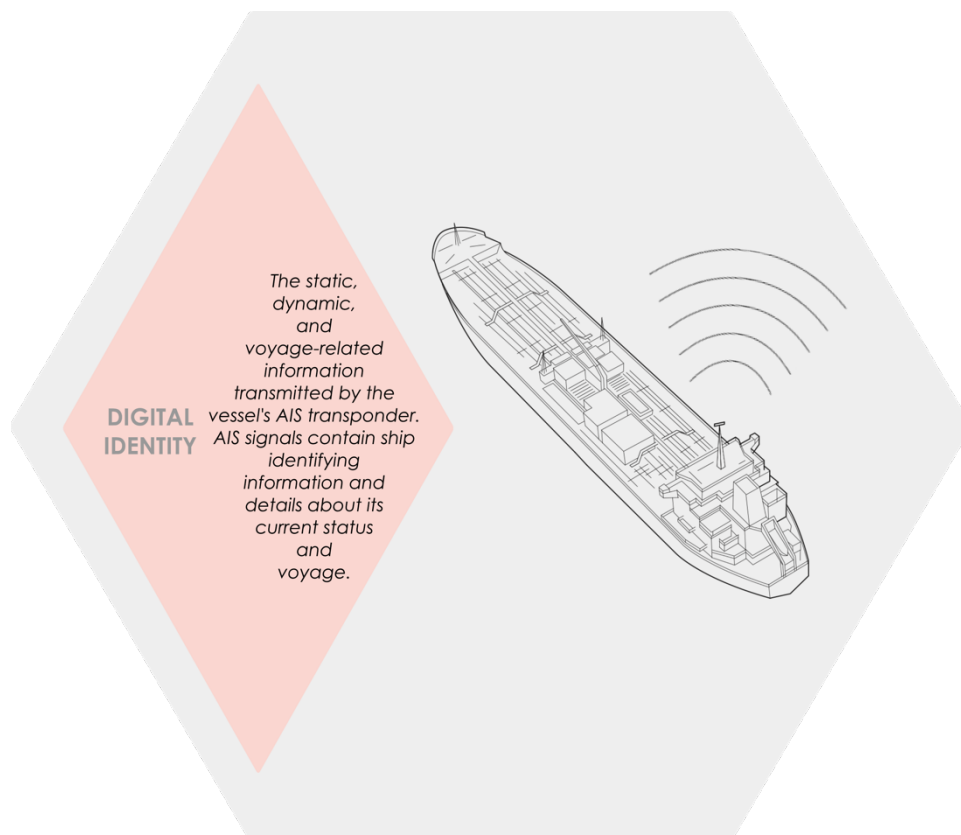
Identifying information that is included in a vessel's IMO-registered identity can include, but is not limited to, the following:

- The vessel's IMO number
- Unique identifiers for communications equipment (e.g. MMSI number and call sign)
- Registered flag

- Ownership and management history
- A vessel's physical dimensions and construction details

Some of this information is self-reported by vessel owners and operators, while other aspects are recorded and reported by maritime authorities, such as flag registries, national governments, and classification societies. The IMO has contracted IHS Markit, a publicly-listed company headquartered in the United Kingdom, to administer the IMO number scheme.¹³ IHS Markit is the only entity authorized to assign and validate IMO numbers, and collects and manages the data for all IMO-registered ships and companies.¹⁴ IHS Markit's databases often serve as the main data source for other public and commercial maritime platforms.¹⁵

DIGITAL IDENTITY

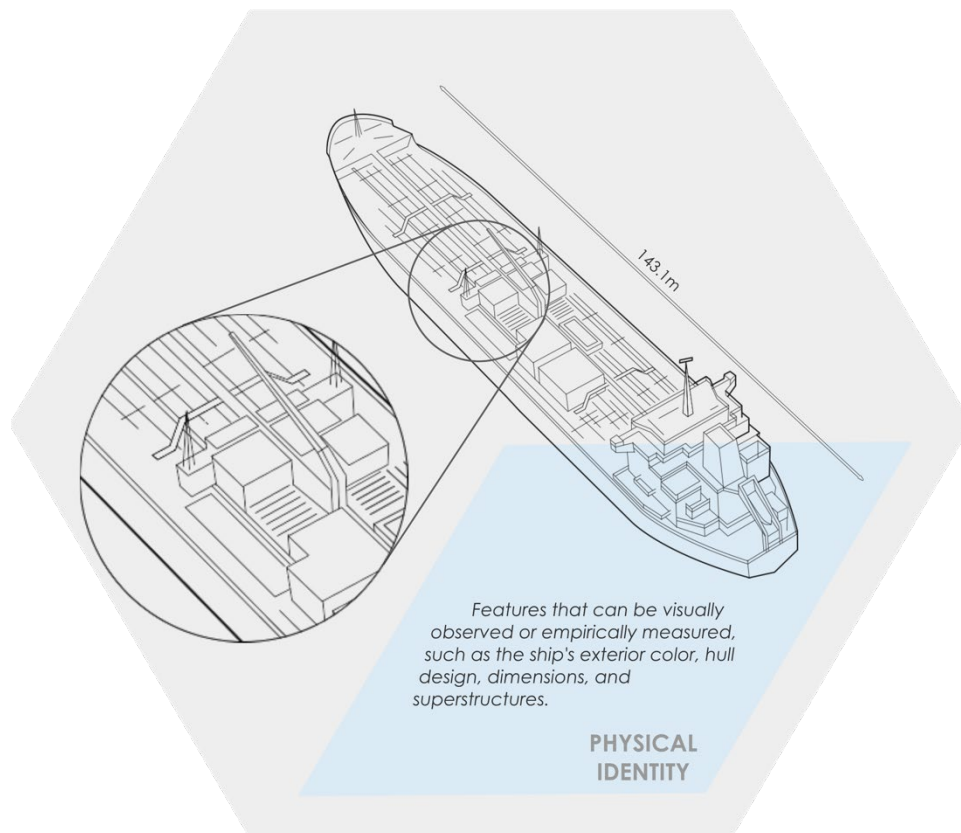


A vessel's digital identity consists of the static, dynamic, and voyage-related information transmitted by the vessel's AIS transponder. Originally designed as a vessel collision avoidance system, the AIS transponder broadcasts the following types of information to surrounding ships and receivers both on land and on satellites.¹⁶

- The ship's identifying information (i.e. "static" information which can include MMSI number, IMO number, call sign, dimensions)
- Dynamic data (e.g. speed, course, rate of turn)
- Voyage details (e.g. destination, estimated time of arrival)

The IMO mandates all vessels of 300 gross tons or more embarking on international voyages and certain other types of vessels to carry an AIS transponder that meets standards defined by the IMO.¹⁷ Vessels that do not fall into those categories, such as leisure crafts and some domestic trading vessels, still often voluntarily carry an AIS transponder for its navigational benefits or are otherwise required to do so according to national regulations. Regardless, AIS transmissions are accessible to anyone with the properly configured receivers or through public and commercial AIS tracking platforms.

PHYSICAL IDENTITY



A vessel's physical identity is determined by features that can be visually observed or empirically measured, including the following:

- Cosmetic (e.g. paint scheme);
- Structural (e.g. hull design, deck configuration, pipelines, engine); and
- Measured (e.g. length and breadth) characteristics.

Two types of imagery help observers establish a vessel's physical identity: satellite or aerial imagery, and ground-level imagery. Satellite or aerial imagery is sometimes available through commercial imagery providers like Planet Labs, Airbus, and Maxar. Ground-level imagery is regularly collected by a global network of ship enthusiasts who regularly capture and upload

photos of vessels to public websites. While satellite, aerial, and ground-level imagery are readily available, tracking the changes to a vessel's physical identity over time can still be a challenge for maritime observers. Some vessels may have been photographed years ago, which may be misleading about the vessel's present-day appearance. Other vessels may have no photographic record at all.

WHAT IS VESSEL IDENTITY TAMPERING?

Vessel identity tampering refers to the deliberate falsification of a vessel's broadcasted data on AIS and/or alterations to its physical features to misrepresent its identity. Vessel identity tampering does not include tampering with a vessel's registered identity, otherwise known as IMO number fraud.

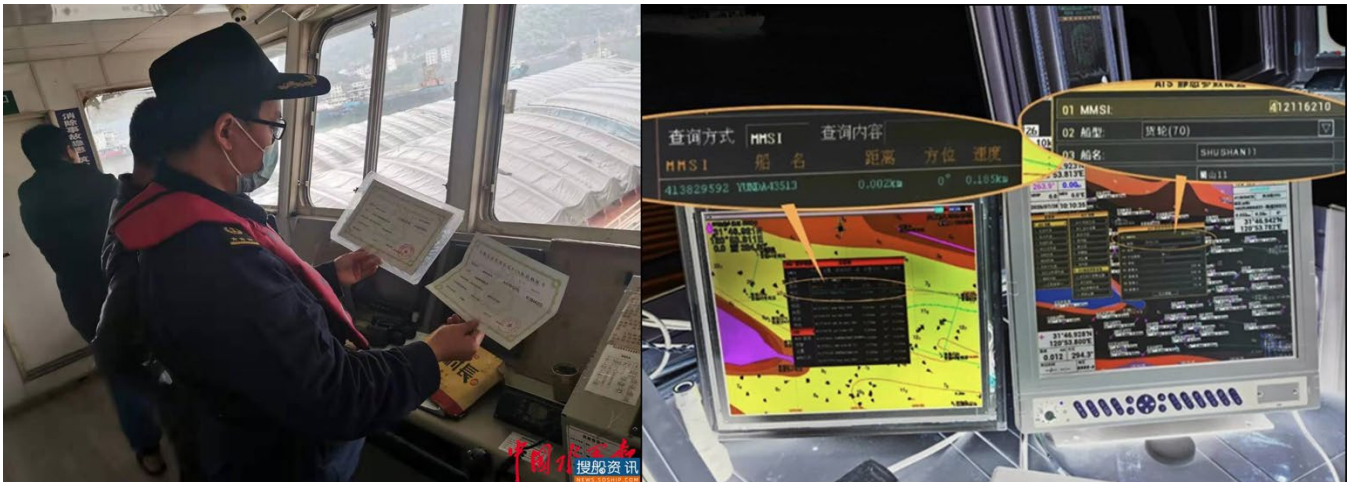
Digital Identity Tampering

Digital identity tampering is the deliberate misrepresentation of a vessel's identity through AIS transponders. A vessel's digital identity is therefore only as secure as its AIS transponder. In order to understand how an AIS transponder can be manipulated, a brief technical discussion of the equipment is needed.

An AIS transponder is linked to a vessel primarily through the Maritime Mobile Service Identity (MMSI) number.¹⁸ The MMSI number is a nine-digit number that is used by maritime communications equipment like AIS transponders to identify a vessel or coast radio station.¹⁹ An AIS transponder can transmit a range of "messages" that carry different information, but the MMSI number is the only vessel identifier included in all positional transmissions.^{20 21} For that reason, the MMSI number allows the vessel to be tracked across individual transmissions over space and time, forming the basis of the vessel's digital identity.

MMSI tampering occurs when a vessel transmits the MMSI number of another vessel or an entirely fraudulent one in order to obfuscate its identity and activities. In effect, MMSI tampering creates new digital identities that severely impair the ability of maritime authorities and other vessels to identify a vessel and monitor its movements.

Although AIS transponders have built-in security features designed to prevent tampering of the MMSI number, they are inconsistent across manufacturers and can be easily circumvented. Depending on the AIS transponder model, the encoded MMSI number can be changed after entering a special passcode supposedly known only to the manufacturer and authorized equipment dealers and technicians. However, these passcodes are not always well-protected, as some can be found in online forums where they are shared openly between frustrated seafarers looking to avoid the costs and time required to send a transponder to a manufacturer for servicing.²² In addition to reprogramming the onboard AIS transponder, a user can also purchase multiple AIS transponders, meaning illicit actors can simply acquire fresh transponders whenever they need to generate new digital identities.



Left: A China Maritime Safety Administration official inspects the ship radio station licenses of a vessel suspected to have broadcasted multiple MMSI numbers (July 2020). Right: Two AIS transponders each programmed with their own MMSI number found onboard a China-flagged cargo ship (November 2020). Source: Soship.com²³; cssglw.com.²⁴

Physical Identity Tampering

Physical identity tampering is the deliberate modification of a vessel's physical appearance in order to disguise itself.

Crews or vessel operators can make cosmetic modifications at sea by painting new identifiers, changing name plates and flags, or covering sections of the deck with tarp. Such rudimentary measures are unlikely to withstand scrutiny from trained observers, but they offer a basic level of physical obfuscation that is low-cost and easy to implement.



Imagery of a DPRK-flagged tanker with fake cargo hatches installed on its deck. Source: UN Panel of Experts.²⁵

More significant cosmetic and structural modifications usually require access to specialized expertise, materials, and equipment that can only be found at shipyards or other onshore facilities. At a shipyard, a vessel can undergo a complete repainting of its deck and hull, make structural alterations to the hull (e.g. lengthening or shortening, adding secret compartments,

converting from one vessel type to another), or reconfigure deck features (e.g. rearranging piping and containers).

The Limits of Identity Tampering

While there is no doubt that identity tampering poses challenges to the detection and investigation of ships engaging in illicit activities, these types of physical or digital identity manipulation are largely superficial. Identity tampering does not attempt to change the vessel's true, registered identity as recorded by the IMO, the *de facto* single source of truth for establishing vessel identities.

A vessel could technically transmit any MMSI number that it wants, but an unregistered radio signal or simultaneous transmission of the same MMSI number with another vessel would draw scrutiny from law enforcement and regulators. Similarly, if a vessel presents a different name and IMO number on its hull, a quick cross-check in maritime databases and AIS platforms can corroborate whether the vessel matches the registered characteristics of its cover identity, and does not exhibit any anomalous AIS transmissions.

Engaging in identity tampering causes the components of a vessel's physical and digital identities to become misaligned with its registered identity, leaving the vessel at greater risk of exposure.

But what if a vessel was able to obtain a new registered identity and IMO number?

A novel tactic called vessel identity laundering exploits vulnerabilities in the IMO number system in order to generate fraudulent IMO numbers that enable vessels to discard their original registered identities and assume new ones. The following section will introduce the concepts behind vessel identity laundering and compare it with vessel identity tampering.

WHAT IS VESSEL IDENTITY LAUNDERING?

Vessel identity laundering, similarly to identity tampering, is the deliberate misrepresentation of a “dirty” vessel's identity as a “clean” one, *but also involves defrauding the IMO to obtain a false registered identity*. Specifically, a vessel identity laundering operation consists of the following elements.

1. One or more ships deliberately tampering or misrepresenting aspects of their physical, digital, and registered identities to obfuscate their original identity;
2. At least one ship taking on a “shell” identity. A shell identity refers to an IMO-registered identity that was obtained under false pretenses, a process also known as IMO number fraud. A shell identity has no authentic connection to a ship.

The idea behind a vessel identity laundering operation is straightforward. When a ship is designated or blacklisted, its identity is compromised, or “dirty,” and laws and regulations prohibit its normal operation. To get around these restrictions, the vessel's operators require a

new, “clean” identity for the ship. A common solution had been to engage in identity tampering tactics, such as painting over the dirty ship's original IMO number or to broadcast a fake MMSI number so that it would not transmit under its own identity on AIS.

Vessel identity laundering, however, goes much further than these elementary schemes to disguise a dirty identity. The masterminds of the operation fabricate a new seemingly legitimate, clean identity—a shell identity—that does not belong to a real vessel, so that it can be used by another ship. In some identity laundering operations, it is the dirty vessel directly uses the shell identity—we call this a direct vessel identity laundering operation. In others, a clean, “intermediary” ship assumes the shell identity, leaving its own original identity to be adopted in turn by a dirty ship—this is called an indirect vessel identity laundering operation. We cover the specifics of each typology in the following chapter of this report.

Vessel Identity Tampering vs. Vessel Identity Laundering

The key difference between vessel identity tampering and vessel identity laundering is the level of sophistication and coordination demonstrated by actors in this operation. Rather than relying on ad hoc identity tampering measures to pass off a dirty ship as a different vessel, the orchestrators of a vessel identity laundering operation go so far as to invest resources into creating fraudulent shell identities. Their subsequent use of this newly fabricated identity requires coordination between the different entities involved to make sure that ships are not broadcasting the same IMO number or MMSI number at the same time. In sum, vessel identity laundering demonstrates high levels of effort, coordination, and use of resources to create and maintain a clean identity for a dirty ship.

Ships involved in vessel identity laundering schemes rarely exhibit the usual telltale signs of AIS tampering or sloppy paint jobs that cover old ship names. As a result, law enforcement and civil regulators have a significantly greater challenge in identifying vessels involved in an identity laundering operation, which requires thorough cross-comparisons between IMO registration data, AIS transmissions across multiple identities, and the physical features of ships as seen in imagery. The technical expertise and data access required to conduct such investigations are considerably higher than what many regulators in the maritime domain are able to harness, and reduce the likelihood that regulators can produce actionable insights with the timeliness required to disrupt illicit activity.

Based on available data and evidence, C4ADS has identified at least two types of vessel identity laundering operations: direct and indirect. The following section will outline typologies for direct and indirect vessel identity laundering using hypothetical scenarios before introducing real-world examples as case studies in subsequent sections. Both types of vessel identity laundering involve IMO number fraud but differ in the number of vessels involved to execute the operation. At the end of each operation, a DPRK-linked, dirty vessel acquires a clean cover identity with which it can evade sanctions and avoid detection.

VESSEL IDENTITY LAUNDERING: TWO TYPOLOGIES

To explain the two different typologies of vessel identity laundering operations, we will use the example of a fictional ship named the SAPPHIRE. We use fictional ship names that correspond to the color of the ship's *original* exterior to help readers track changes to a vessel's identity.

In these scenarios, the SAPPHIRE, which has been issued the IMO number 1234567, is a ship that was designated by the UNSC and OFAC for violating sanctions on the DPRK. The designation of the vessel presents many operational challenges for the SAPPHIRE's owners and operators. The vessel is blacklisted by financial institutions and flag registries are unwilling to issue the ship with a new registration. Additionally, the ship is subject to a global port entry ban, limiting the utility of the ship. The operators decide that the SAPPHIRE, whose identity is "dirty" from its designation, requires laundering to become "clean."

In the previous section, we defined vessel identity laundering as an operation that involves the following two elements:

- One or more ships broadcasting a digital identity different to their own;
- Existence of a "shell" identity (an IMO-registered ship identity that was fraudulently obtained under false pretenses).

We will consider the hypothetical cases of "direct" and "indirect" vessel identity laundering below.

TYPE 1: DIRECT VESSEL IDENTITY LAUNDERING OPERATION

A direct vessel identity laundering operation typically follows a three-step process and only requires one real ship (the dirty vessel itself):

Step 1 Preparation and Disguise: Physical Identity Tampering

The dirty ship undergoes physical modifications and other methods to hide its original identity, such as painting over its own IMO number.

In many cases, the dirty ship is physically modified in order to facilitate the next step of applying for a fraudulent IMO number. For instance, the ship may be modified to look like a newly built ship on the surface, or to look like a different ship that has never registered with the IMO before (e.g. because it has never sailed internationally).

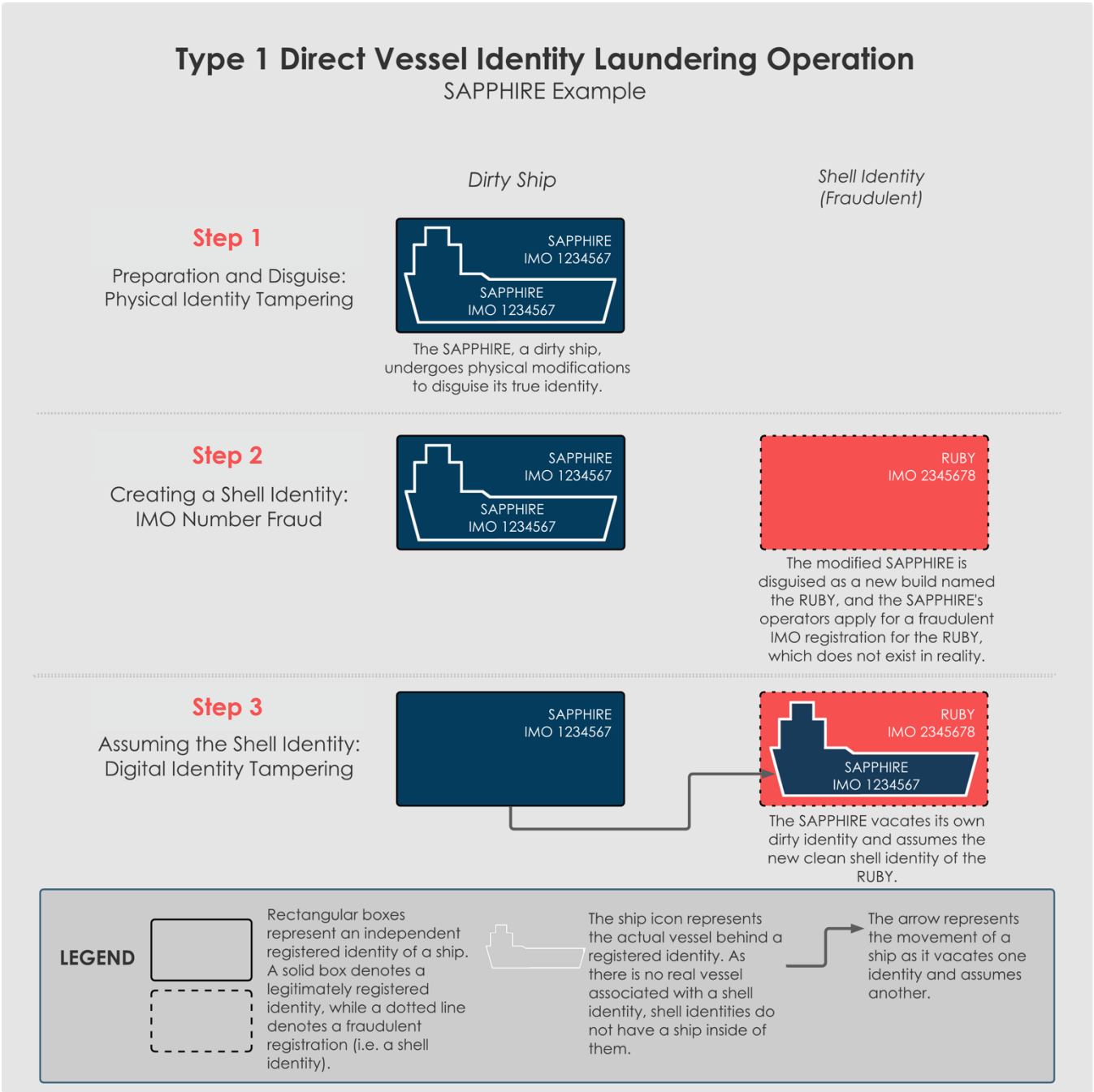
Step 2 Creating a Shell Identity: IMO Number Fraud

The orchestrators of the operation defraud the IMO into issuing a shell identity.

Step 3 Assuming a Shell Identity: Digital Identity Tampering

The dirty vessel stops transmitting AIS under its original identity and transmits under this newly obtained shell identity instead to appear clean.

We explain these steps in greater detail below.



Step 1 Preparation and Disguise: Physical Identity Tampering

The SAPPHIRE's operators send the ship to a shipyard to be repainted. In addition to having its original IMO number painted over to hide its identity, the ship's hull and deck, which were formerly blue, are painted over in red. This is meant to change the ship's physical appearance and disguise the ship from those who may recognize the SAPPHIRE from its original blue exterior.

In addition to giving the SAPPHIRE a fresh coat of paint, the shipyard paints a new name, the "RUBY," onto the SAPPHIRE's hull, and provides documents falsely stating that the so-called RUBY—which of course, is the SAPPHIRE in reality—is a ship that has been newly constructed at the shipyard.

Step 2 Creating a Shell Identity: IMO Number Fraud

The SAPPHIRE's operators apply for a new IMO number for the RUBY. In this application, the operators include photographs taken of the SAPPHIRE disguised as the RUBY as proof of the RUBY's existence. Of course though, the RUBY is not a real vessel because the actual ship that is posing as the RUBY is the SAPPHIRE.

Recall that the SAPPHIRE already has an IMO number. A vessel's IMO number is supposed to last through its lifetime, so the SAPPHIRE is clearly not eligible for another IMO registration, regardless of whether it has changed its name or appearance. However, in this case, the SAPPHIRE's operators are falsely representing the so-called RUBY as a newly built ship in its IMO number application. From the IMO's perspective, there is nothing strange about this request, because naturally, a new ship does not have an IMO number until it is registered with the IMO.

The IMO assesses the documents included in the ship's application, such as the vessel details and certificates issued by the shipyard, and approves the ship's registration. The IMO assigns the IMO number 2345678, for the ship that they believe is the newly built RUBY. At this point, the RUBY, despite not actually existing, has a registered identity with the IMO. However, unlike real ships that are issued an IMO number, the IMO-registered RUBY identity does not belong to an actual ship and exists in records only. In other words, it is an empty shell.

Step 3 Assuming the Shell Identity: Digital Identity Tampering

With the RUBY identity having been successfully registered with the IMO, the SAPPHIRE is now able to assume the clean RUBY identity.

The SAPPHIRE first vacates its original digital identity by turning off the AIS transponder onboard the ship that was broadcasting the SAPPHIRE's identifiers on AIS.

Next, the SAPPHIRE assumes the identity of the RUBY by configuring an AIS transponder onboard to transmit the RUBY's identifiers. These AIS transmissions

appear as if they are coming from a vessel called the RUBY, which has the IMO number 2345678. However, as we are aware, the ship that is broadcasting AIS using this identity, is actually the SAPPHIRE (IMO 1234567).

The vessel identity laundering operation is complete. In all instances of official declaration of its identity, whether on paper (registered identity), on AIS (digital identity), or through the name and IMO number painted onto the ship (physical identity), the vessel that used to be known as the SAPPHIRE (IMO 1234567) now presents itself as the RUBY (IMO 2345678).

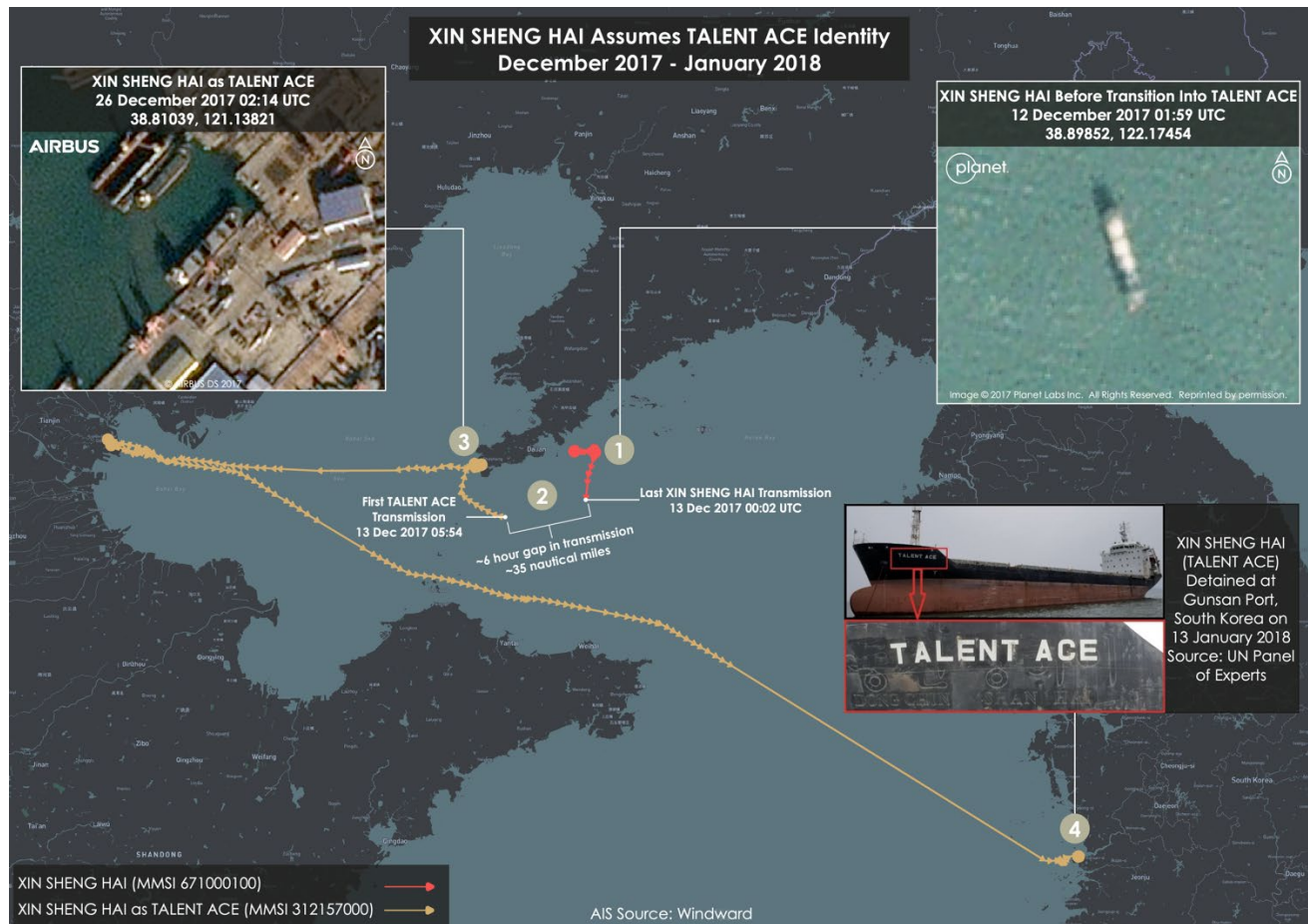
Mini Case Study

THE FIRST REPORTED CASE OF VESSEL IDENTITY LAUNDERING: THE TALENT ACE

The first reported case of DPRK-linked vessel identity laundering was a direct vessel identity laundering operation involving the XIN SHENG HAI (IMO 9485617), a formerly Belize-flagged cargo ship that allegedly exported DPRK-origin coal in violation of UN sanctions in August and September 2017.²⁶ On 13 January 2018, South Korean authorities detained the vessel after it entered Gunsan Port while using a fraudulent IMO-registered identity as the Togo-flagged cargo ship TALENT ACE (IMO 8793873).²⁷

The Panel's investigation of the case revealed how the network behind the XIN SHENG HAI manipulated its registered, digital, and physical identities. Authorities discovered ship documents onboard indicating that the network attempted to pass the TALENT ACE off as a first-time applicant for an IMO number. Maritime databases show that the TALENT ACE identity was likely customized for the XIN SHENG HAI in order to build a more convincing profile; the TALENT ACE was registered with the same gross tonnage and its year of build was listed as one year before that of the XIN SHENG HAI. On board the ship, investigators found the fraudulent IMO number and name affixed to the vessel's superstructure and hull. A review of the TALENT ACE's and XIN SHENG HAI's AIS transmission histories shows that the XIN SHENG HAI assumed the TALENT ACE's identity on 14 December 2017—only six hours after the XIN SHENG HAI ceased broadcasting its own IMO number and original registered identifiers.

Although the TALENT ACE identity laundering operation ultimately failed to fool government authorities, the vessel appeared to have secured shipping and financial services during the one-month period it sailed under the identity. After the South Korean authorities detained the TALENT ACE, the crew was reportedly abandoned in South Korea, leading the International Labor Organization (ILO) to open an abandoned seafarer case for the vessel. Case notes by the investigator noted that the vessel may have obtained financial services from a German protection and indemnity (P&I) club. In addition to obtaining a Togo flag registration, the vessel also reportedly received classification services from an Asian recognized organization.²⁸



AIS data and imagery show the XIN SHENG HAI's transition into the fraudulent TALENT ACE identity in December 2017. Source: Imagery provided by Planet Labs, Airbus Defence and Space; AIS data provided by Windward; UN Panel of Experts.

Nearly three-and-a-half years after its detention in Gunsan Port, South Korean authorities began scrapping the TALENT ACE in mid-2021.²⁹ However, as we will see in the case studies later in this report, other DPRK-linked shipping networks have engaged in even more sophisticated vessel identity laundering operations that deceived the international community for years.

TYPE 2: INDIRECT VESSEL IDENTITY LAUNDERING OPERATION

Indirect vessel identity laundering operations are more complex than direct vessel identity laundering operations. While direct vessel identity laundering requires only one vessel, indirect vessel identity laundering operations require the participation of at least two real ships (including the dirty vessel and a clean “intermediary” vessel). However, the goal is still the same: to provide the dirty vessel with a clean identity.

Indirect vessel identity laundering operations typically follow a four-step process:

Step 1 Preparation and Disguise: Physical Identity Tampering. Vessel operators seek to create a fraudulent identity for a dirty vessel to assume. However, in indirect vessel identity laundering operations, a clean intermediary vessel is used in the first step, rather than the dirty vessel. The intermediary ship undergoes physical modifications and other methods to hide its original identity.

In many cases, the intermediary ship is modified in a way to facilitate the application for a fraudulent IMO number, such as being disguised to look like a newly built ship, or a different ship that has never registered with the IMO before.

Step 2 Creating a Shell Identity: IMO Number Fraud

The orchestrators of the operation defraud the IMO into obtaining a shell identity.

Step 3 The Intermediary Ship Assumes the Shell Identity: Digital Identity Tampering

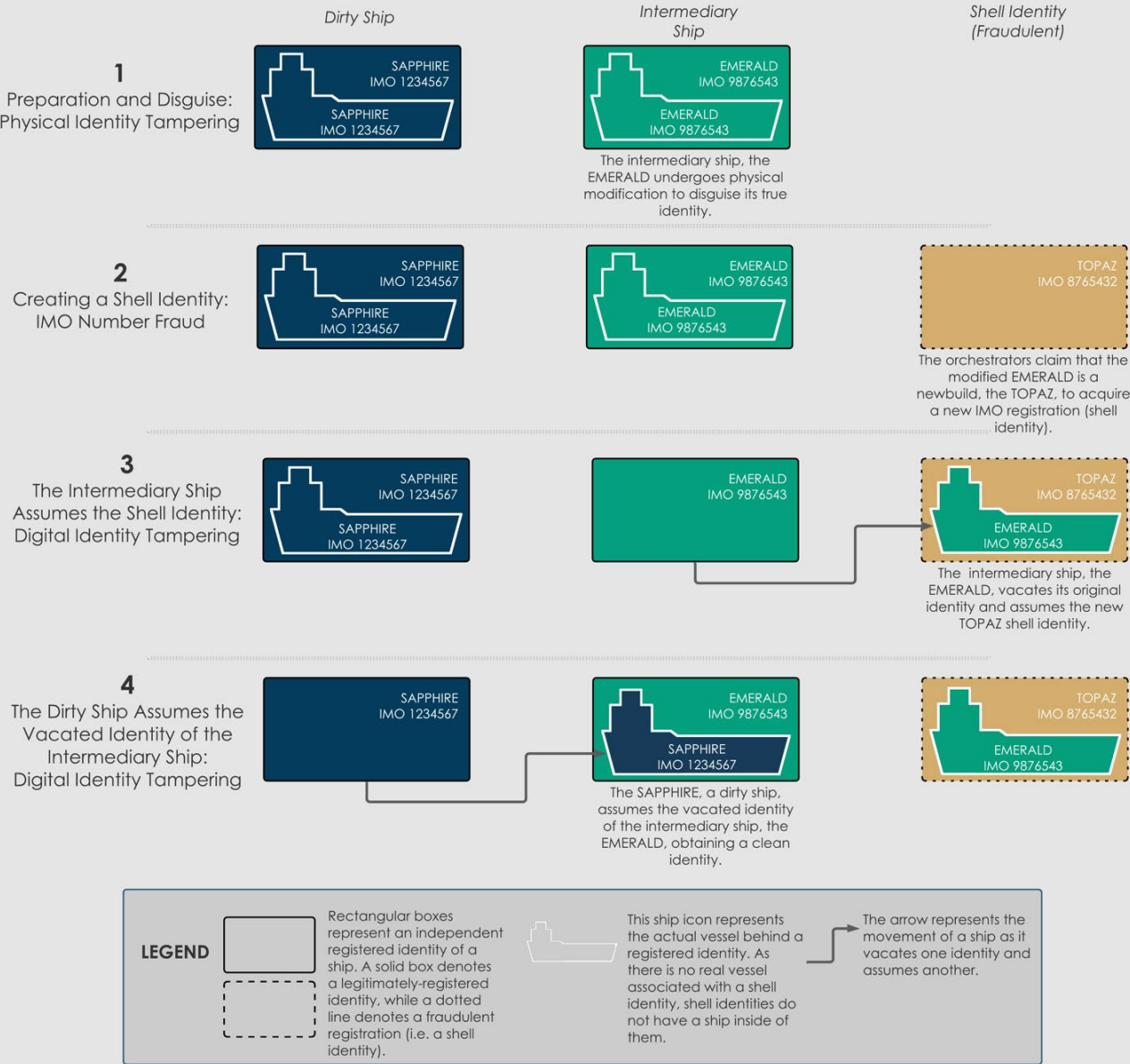
The intermediary vessel stops transmitting AIS under its original identity, and assumes the shell identity on AIS, vacating its original identity.

Step 4 The Dirty Ship Assumes the Vacated Identity of the Intermediary Ship: Digital Identity Tampering

The dirty ship assumes the now-vacated identity of the intermediary vessel and transmits the intermediary vessel's identifiers, making it appear clean.

Let's go back to the example of the SAPPHIRE to see how this works.

Type 2 Indirect Vessel Identity Laundering Operation
SAPPHIRE Example



Step 1 Preparation and Disguise: Physical Identity Tampering

The SAPPHIRE, just like in the first example, is the dirty vessel that requires a new, clean identity to operate. However, in indirect vessel identity laundering operations, the dirty vessel is not involved in the identity laundering operation at this stage.

Instead, the first three steps involve an intermediary ship. In our example, the intermediary ship will be called the EMERALD. The EMERALD, which has been issued the IMO number 9876543, has similar physical dimensions to the SAPPHIRE. It has never been implicated in any illicit activity. In other words, it is a clean ship whose registered identity and verifiable history would serve as a good cover identity for the SAPPHIRE after a few modifications to make it look the part.

The EMERALD, which has a green hull, is sent to a shipyard for repainting. Its hull is painted over in yellow, all of its original IMO number markers are painted over, and the ship is emblazoned with the fraudulent name "TOPAZ".

Step 2 Creating a Shell Identity: IMO Number Fraud

From here, the EMERALD's operators apply for an IMO registration for the TOPAZ using fraudulent documents that claim that the TOPAZ is a newly built ship. The operators submit pictures of the EMERALD with its hull painted yellow and the name "TOPAZ" shown on its stern as part of its IMO application. The IMO, duped by falsified documents and unable to recognize the ship in the pictures as the IMO-registered EMERALD, issues an IMO number for the TOPAZ (IMO 8765432).

Step 3 The Intermediary Ship Assumes the Shell Identity: Digital Identity Tampering

The EMERALD first vacates its own digital identity by turning off the AIS transponder onboard the ship. Next, the EMERALD assumes the identity of the TOPAZ by configuring an AIS transponder onboard to transmit the TOPAZ's identifiers. These AIS transmissions appear as if they are coming from a vessel called the TOPAZ, which has the IMO number 8765432. However, as we are aware, the ship that is broadcasting the AIS using this identity is actually the EMERALD.

Step 4 The Dirty Ship Assumes the Vacated Identity of the Intermediary Ship: Digital Identity Tampering

Now that the EMERALD's digital identity is vacant, the SAPPHIRE, a dirty ship, can assume the EMERALD's clean identity. To do so, the SAPPHIRE first vacates its own digital identity by turning off the AIS transponder onboard the ship. Next, the SAPPHIRE assumes the identity of the EMERALD by configuring its onboard AIS transponder to transmit the EMERALD's identifiers.

The vessel identity laundering operation is complete. In all instances of official declaration of its identity, whether on paper (registered identity), on AIS (digital identity), or through the name and IMO number painted onto the ship (physical identity), the vessel that used to be known as the SAPPHIRE (IMO 1234567) now presents itself as the EMERALD (IMO 9876543), while the EMERALD now presents itself as the TOPAZ.

This typology is different from direct vessel identity laundering operation, because the dirty ship does not assume the fabricated shell identity. However, the end result is the same—the orchestrators defraud the IMO into issuing a shell identity. This extra IMO number allows a dirty ship to assume an identity that is clean.

DIRECT VS. INDIRECT VESSEL IDENTITY LAUNDERING OPERATIONS

Above, we demonstrated two typologies for vessel identity laundering operations involving the fictional SAPPHIRE how a dirty ship is able to disguise itself as a clean one. Real examples of vessel identity laundering operations that C4ADS has observed to date have demonstrated varying levels of complexity and sophistication, but they all ultimately fall into one of these two types. While the two types of vessel identity laundering operations in these examples achieved the same end goal, there are two notable differences in their characteristics.

Direct vs. Indirect :As mentioned above, in Type 1 direct vessel identity laundering, the dirty ship is the direct user of the shell identity. On the other hand, in Type 2 indirect vessel identity laundering, an intermediary ship assumes the shell identity, and its vacated identity is subsequently adopted by the dirty ship, which had no direct involvement with the shell identity.

Single vs. Multiple Real Vessels: Type 1 direct vessel identity laundering only requires one real ship—the dirty ship itself—to undergo the shell identity creation and use. Type 2 indirect vessel identity laundering requires at least two ships: the intermediary ship and the dirty ship.

Additionally, in the 11 cases of vessel identity laundering investigated by C4ADS to date, analysts have observed that shell identities tend to be customized to closely resemble the registered characteristics of the real ship that is its intended user. In contrast, the vacated identity created by an intermediary ship adopting a shell identity in indirect vessel identity laundering operations do not always appear to be customized for the dirty ships that use those identities, and some of these identities have been used by multiple dirty ships.

VARIATIONS IN VESSEL IDENTITY LAUNDERING OPERATIONS

The two above typologies for vessel identity laundering operations are rough, simple examples of vessel laundering operations and may not be comprehensive of all types of laundering operations. In reality, vessels may not take such a linear, step-by-step approach to the operation, or they may find alternative solutions to problems.

For example, there are likely other methods of creating a shell identity that do not require physically disguising a dirty or intermediary ship *before* applying for an IMO number. It is possible that the orchestrators of a vessel identity laundering operation may present photos of a different vessel or ones that were digitally altered when they are required to confirm the physical identity of the applicant ship. In any case, there is still an incentive to establish early in the IMO number registration process that the physical identity of the applicant ship is that of the disguised dirty/intermediary ship. This would likely enhance the credibility of the shell identity and reduce the likelihood of exposure due to discrepancies in physical appearance.

In the following section, we explore the identity laundering operations of the KINGSWAY and SUBBLIC, which are each examples of direct and indirect vessel identity laundering respectively.

Through these case studies, we trace how the operators of two DPRK-linked ships with dirty identities took steps to launder their vessels' identities, allowing them to continue their commercial operations for years before they were detected.

Case Study

TYPE 1 DIRECT VESSEL IDENTITY LAUNDERING: THE KINGSWAY

On the early morning of 6 May 2021, an oil tanker transmitting as the Mongolia-flagged SHUN FA (IMO 8528864) entered the anchorage area of Busan Port, South Korea for a crew change, only to be suddenly detained and boarded by South Korean authorities.³⁰ No one was supposed to know that the SHUN FA was in fact the KINGSWAY (IMO 9191773), a vessel sanctioned by the UN Security Council since 2017.³¹

This case study will outline how the KINGSWAY underwent a vessel identity laundering operation to adopt a “clean” identity, which it used to sail under the radar of international sanctions monitors for approximately three years. The case of the KINGSWAY is a complex variation of two Type 1 direct vessel identity laundering operations that occurred simultaneously. The KINGSWAY and TWINS BULL (IMO 9106340) were “dirty” ships managed by the same network that were accused of transferring fuel to North Korean tankers in 2017.³² Each underwent separate identity laundering operations that were executed in close coordination.



The fraudulent name (SHUN FA) and IMO number (8528864) were painted on the KINGSWAY, pictured above in Busan Port, South Korea on 18 August 2021. Source: Photos courtesy of NK News.³³

KINGSWAY and TWINS BULL Vessel Identity Laundering Operation

Direct Vessel Identity Laundering Operation into the APEX/SHUN FA and W STAR

Step 1

Preparation and Disguise:
Physical Identity Tampering
January 2018

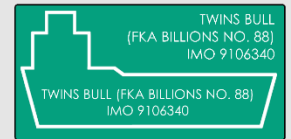


The KINGSWAY was sanctioned by the UNSC for transferring oil to DPRK interests in violation of UN sanctions. The ship underwent physical modifications to disguise its identity.

Shell Identity
(Fraudulent)

Shell Identity
(Fraudulent)

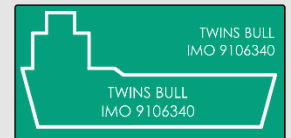
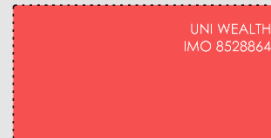
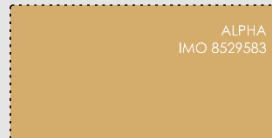
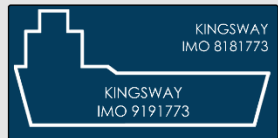
Dirty Ship



The TWINS BULL was also accused of transferring oil to North Korean tankers. The ship underwent physical modifications to disguise its identity.

Step 2

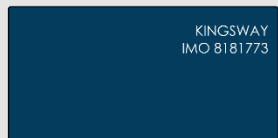
Creating a Shell Identity:
IMO Number Fraud
February - July 2018



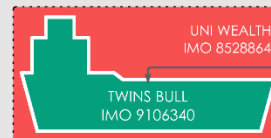
Through IMO fraud, the KINGSWAY network successfully obtained two shell identities, the ALPHA and UNI WEALTH, for laundering the identities of the KINGSWAY and TWINS BULL.

Step 3

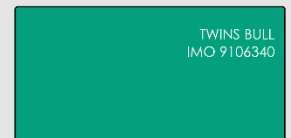
Assuming the Shell Identity:
Digital Identity Tampering
July 2018



The KINGSWAY vacated its original identity on AIS and assumed the ALPHA identity on AIS.

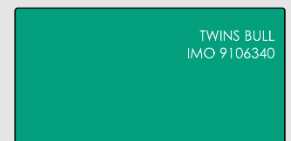
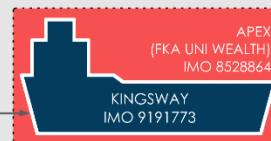
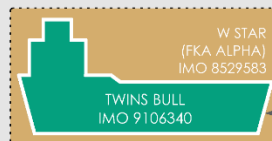
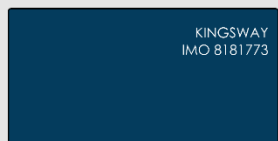


Similarly, the TWINS BULL vacated its original identity and assumed the UNI WEALTH digital identity on AIS.



Step 4

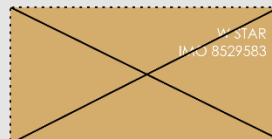
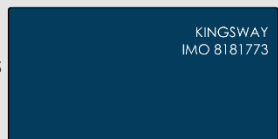
The Swap:
Reassigning Shell Identities
October - November 2018



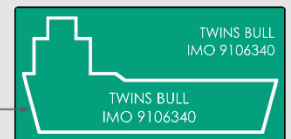
Likely in an attempt to match the recorded dimensions of the shell identities with the dimensions of the real vessels transmitting them, the operators of the KINGSWAY and TWINS BULL swapped shell identities between the KINGSWAY and TWINS BULL, so that the KINGSWAY assumed the APEX (FKA UNI WEALTH) identity, and the TWINS BULL assumed the W STAR (FKA ALPHA) identity.

Aftermath

Deregistration of the W STAR and the TWINS BULL's Return to its Original Identity
April 2020



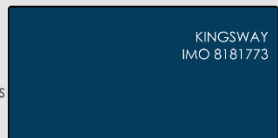
The IMO deregistered the W STAR identity after finding out that the registration was made under false pretenses.



The TWINS BULL lost its cover identity and returned to its original identity on AIS.

Aftermath

The KINGSWAY Sails Under the APEX Identity for Three Years Before its Detention
November 2018 - Present

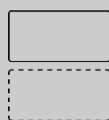


The KINGSWAY remained undetected sailing under the fraudulent registered identity of the APEX/SHUN FA until May 2021. During this time, the ship has often shown sailing patterns indicative of fuel smuggling.



The TWINS BULL (NKA RUGUN LATA) has not shown signs of suspicious activity since it reverted back to its original identity.

LEGEND



Rectangular boxes represent an independent registered identity of a ship. A solid box denotes a legitimately registered identity, while a dotted line denotes a fraudulent registration (i.e., a shell identity).



The ship icon represents the actual vessel behind a registered identity. As there is no real vessel associated with a shell identity, shell identities do not have a ship inside of them.



The arrow represents the movement of a ship as it vacates one identity and assumes another.

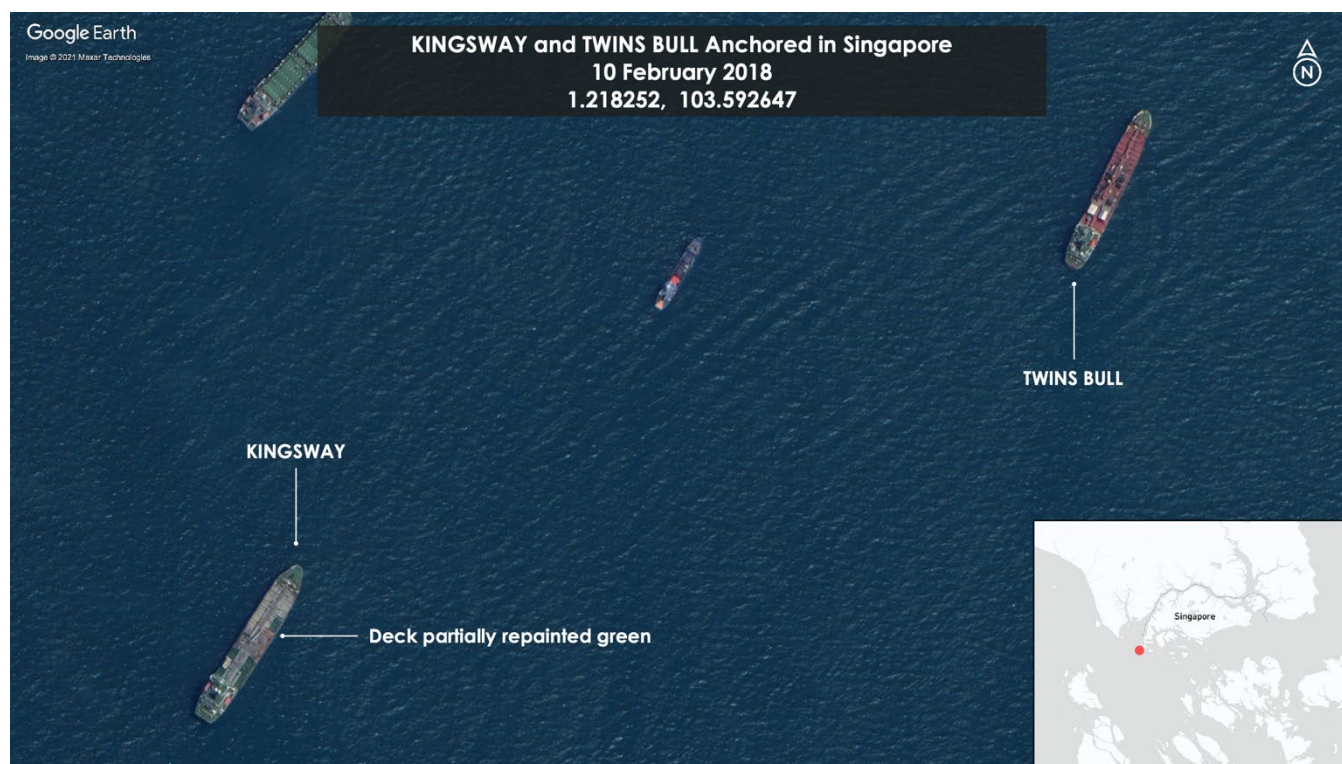
Step 1 Preparation and Disguise: Physical Identity Tampering

The KINGSWAY (then known as the BILLIONS NO. 18) was sanctioned by the UN Security Council (UNSC) in December 2017 for transferring fuel through a ship-to-ship (STS) transfer to a North Korean tanker.³⁴ As a result of its designation, the KINGSWAY was banned from entering ports worldwide.³⁵

In January 2018, the KINGSWAY and TWINS BULL attempted to enter Kaohsiung Port, Taiwan. However, the ships were denied entry by Taiwan authorities at the request of the UNSC.³⁶

A few days after this event, the KINGSWAY and TWINS BULL sailed southwest into the South China Sea, where both vessels disappeared. The KINGSWAY has never transmitted AIS signal under its own identity since then. The TWINS BULL did not transmit AIS under this identity again until two years later. We will return to why later in this case study.

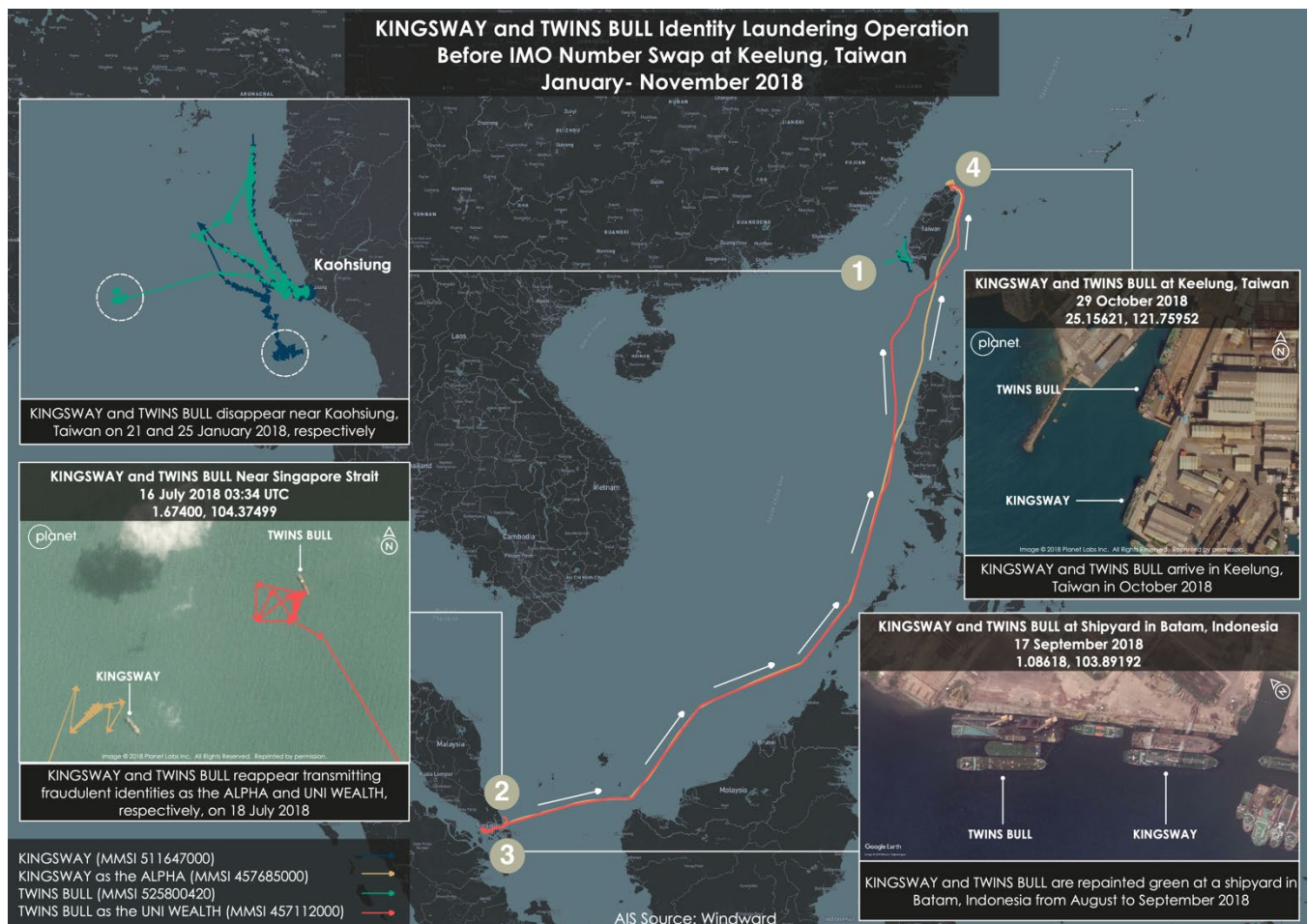
Satellite imagery shows that the KINGSWAY and TWINS BULL fled to Singapore, where they were observed to be anchored from at least February to May 2018. Neither vessel appears to have broadcast AIS signal during this period, possibly in order to hide their locations and identities in preparation for an identity laundering operation. Over the next few months, the KINGSWAY and TWINS BULL took steps to modify their physical appearances. The image below, captured on 10 February 2018, shows the KINGSWAY's formerly grey deck in the process of being repainted green.



The KINGSWAY and TWINS BULL anchored in Singapore after being kicked out of Taiwanese waters. Source: Google Earth, Maxar Technologies.

The operators of the KINGSWAY and TWINS BULL then likely submitted fraudulent documents to the IMO to apply for the registration of two Mongolia-flagged ships: the ALPHA (IMO 8529583) and UNI WEALTH (IMO 8528864).

Step 3 Assuming the Shell Identity: Digital Identity Tampering



30

The KINGSWAY and the TWINS BULL first transmitted the identities of the ALPHA and UNI WEALTH, respectively, on AIS while anchored northeast of the Singapore Strait in July 2018.

Having assumed their new digital identities, the vessels' next step was to further enhance their physical disguises through repainting. This would allow the ships to distance themselves even more from their original appearances as the KINGSWAY and TWINS BULL.

From August to September 2018, the KINGSWAY and TWINS BULL were likely repainted at a shipyard in Batam, Indonesia. Satellite imagery shows both the formerly grey deck of the KINGSWAY and red deck of the TWINS BULL were fully painted over in green.

Following their repainting, the identity laundering operations for both ships were seemingly complete. The KINGSWAY and TWINS BULL had acquired and adopted clean, shell identities of the ALPHA and UNI WEALTH, and both vessels had also undergone physical modifications to look the part. Even though the vessels were already sailing under laundered identities, the vessels' operators took an extra step to further distance each vessel's actual identity from its fraudulent one.

Step 4 The Swap: Reassigning Shell Identities

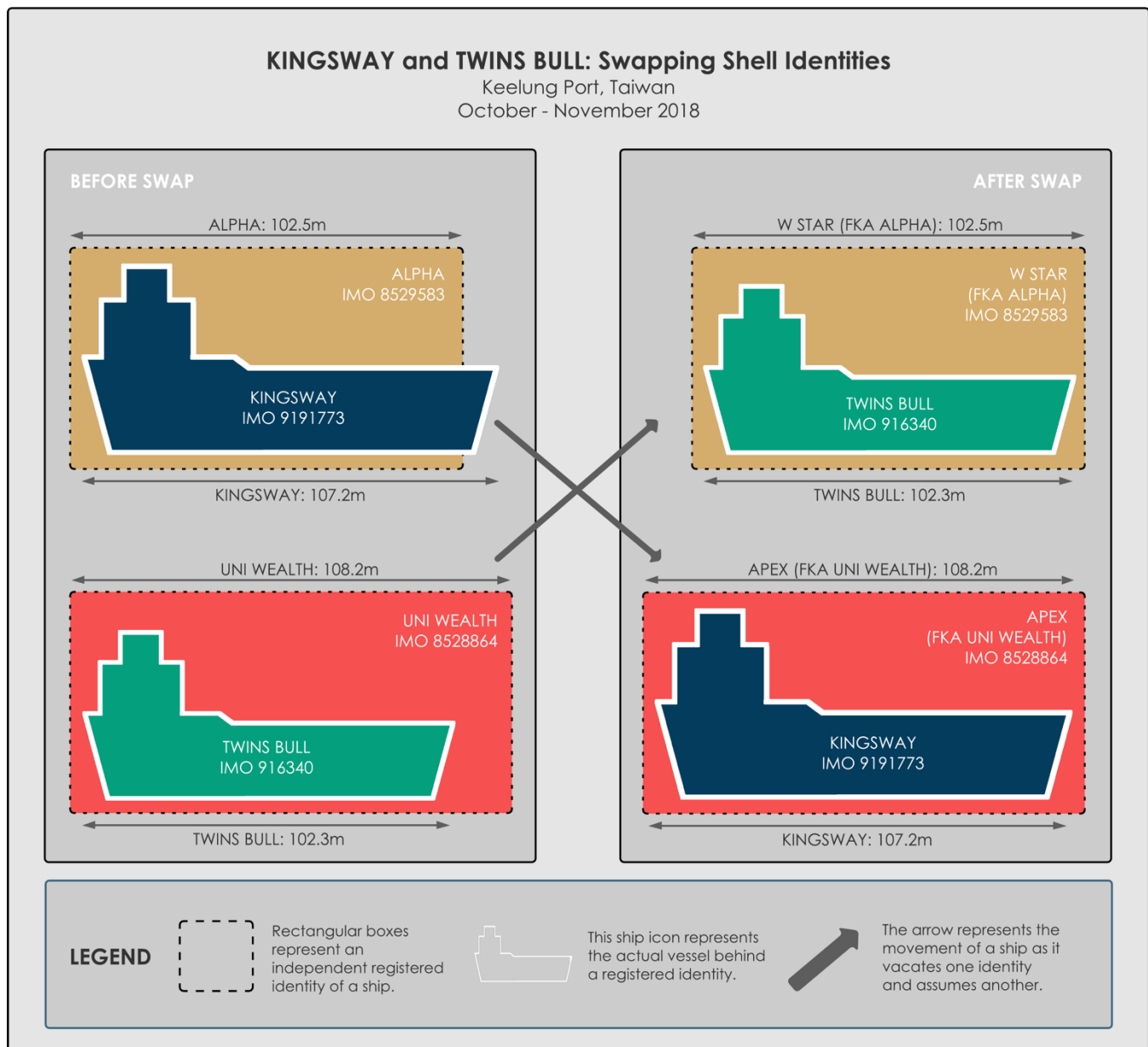
Normally, a direct identity laundering operation is complete after the dirty ship adopts the shell identity, like the KINGSWAY and TWINS BULL did when they assumed the ALPHA and UNI WEALTH identities respectively. However, soon after the vessels were repainted in Batam, the KINGSWAY and UNI WEALTH sailed to Keelung Port, Taiwan in October 2018, where they did something unusual: the two ships swapped *fraudulent identities with each other*.

Between 29 October and 2 November 2018, the following changes in AIS transmissions were observed from the two vessels:

- The KINGSWAY ceased transmitting, or “vacated,” the ALPHA identity and began transmitting as the APEX, the new name of the UNI WEALTH (IMO 8528864) identity.
- The TWINS BULL vacated the UNI WEALTH identity, and began transmitting as the W STAR, the new name of the ALPHA (IMO 8529583) identity.

This is not normal in either general shipping practices or other cases of vessel identity laundering observed by C4ADS analysts. Not only did the vessels exchange fraudulent IMO numbers, they even briefly transmitted the same IMO number (8529583) for two days during the operation. The vessels' actions carried a high risk of detection by authorities. So why did the operators of the ships do this?

While we cannot speak for the masterminds behind this operation, our investigation suggests that this swapping of IMO numbers may have been executed because the first shell identities used by the KINGSWAY and TWINS BULL were assigned incorrectly.



As shown in this above visualization, prior to the swap, the KINGSWAY's registered length of 107.2 meters is 5 meters longer than the ALPHA's registered length.³⁸ On the other hand, the TWINS BULL is approximately 6 meters shorter than the UNI WEALTH's registered length. In other words, the longer of the two ships was using the shorter of the two registered identities, and vice versa. From the perspective of the vessel identity launderers, the UNI WEALTH's registered length of 108 meters would be a closer and more convincing match for the KINGSWAY, as would the ALPHA be for the TWINS BULL.

Therefore, the swap between the shell identities of the KINGSWAY and TWINS BULL may have occurred to "correct" these discrepancies, and better match the shell identities with the ships using them. As shown above, the two vessels "fit" more closely with their shell identities in the right-side box showing the ships after the swap.

Aftermath

Deregistration of the W STAR and the TWINS BULL's Return to its Original Identity

After trading the two ships' shell identities, the vessel identity laundering operations were complete. These dirty ships now sailed under new identities as they resumed commercial operations.

However, the TWINS BULL was ultimately exposed after sailing for over a year under the fraudulent W STAR identity, which was deregistered in May 2020.³⁹

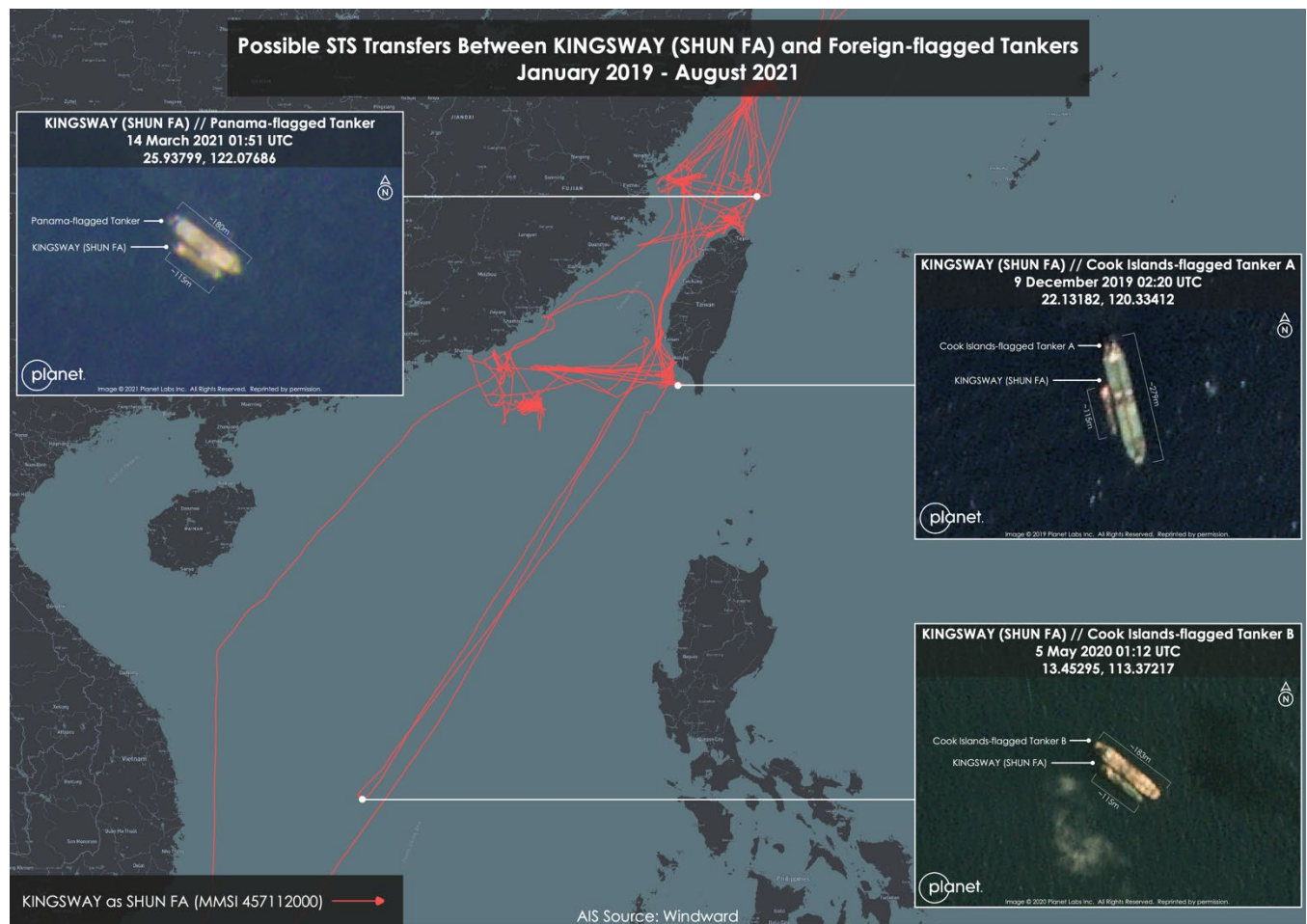
After the two ships switched identities at Keelung Port and the vessel identity laundering schemes were complete, the KINGSWAY and TWINS BULL parted ways. From here, the TWINS BULL, sailing under its new W STAR identity, engaged in shipping patterns that are characteristic of fuel smuggling activity. It did this for over a year, until the vessel was sold to an Indonesian company in March 2020 and renamed as the "RUGUN LATA."⁴⁰ In May of that year, IMO databases indicate that the W STAR's fraudulently obtained IMO number was found to have been registered under false pretenses and its status was changed to "never existed."⁴¹ In July 2020, the TWINS BULL, now known as the RUGUN LATA, reverted back to transmitting its own registered IMO number, ending two years of sailing under shell identities.



Photos of the RUGUN LATA from social media. Source: Facebook.

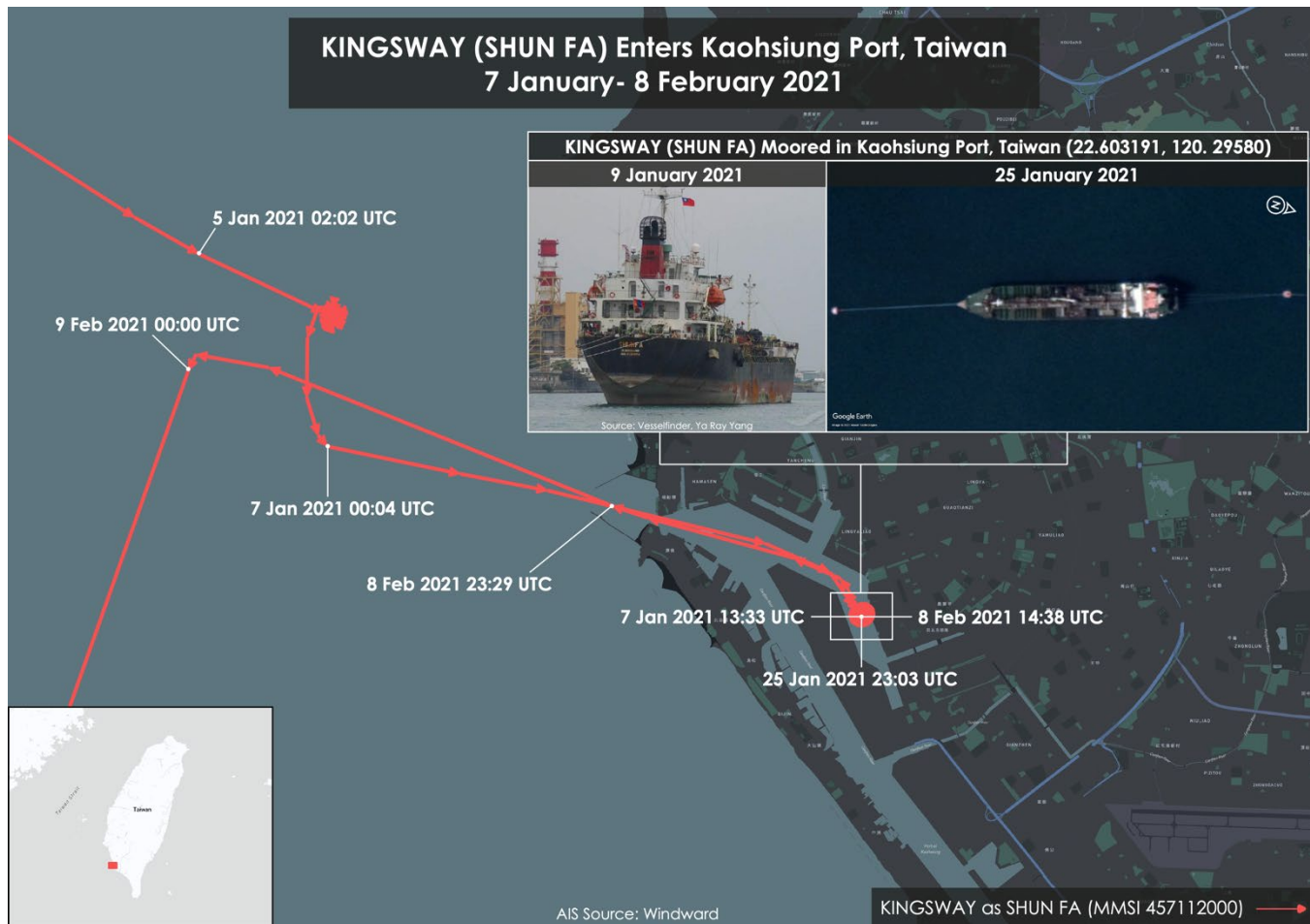
The KINGSWAY Sails Under the APEX Identity for Three Years Before Its Detention

After leaving Keelung under its APEX cover identity, the KINGSWAY also resumed conducting voyage patterns typical of vessels engaging in fuel smuggling. According to AIS data, the vessel embarked on repeated dark voyages near known fuel smuggling hotspots and satellite imagery suggests the vessel likely engaged in several ship-to-ship (STS) transfers with other tankers. In November 2019, the ship changed its name on AIS from the APEX to the SHUN FA, although IMO records continue to list the ship's name as the APEX.



After assuming the APEX/SHUN FA identity, the KINGSWAY continued to conduct STS transfers with other foreign-flagged tankers.⁴² Source: Imagery provided by Planet Labs; AIS data provided by Windward.

Exemplifying the success of its identity laundering operation, the KINGSWAY called at Kaohsiung Port as recently as January 2021—the same port from which the vessel had been turned away three years prior.



Three years after its expulsion from Taiwanese waters, the KINGSWAY returned to Kaohsiung Port, Taiwan under the fraudulent SHUN FA identity in January 2021 where it anchored for a month. Source: Photo provided by Vesselfinder (Photographer: Ya Ray Yang)⁴³; Imagery provided by Google Earth and Maxar Technologies; AIS data provided by Windward.

Ordinarily, providing services to or trading with a sanctioned vessel like the KINGSWAY would render entities vulnerable to prosecution and secondary sanctions risk. However, the KINGSWAY's sophisticated identity laundering operation would provide its trading partners and facilitators with plausible deniability. If a ship looks like the SHUN FA, transmits as the SHUN FA on AIS, and has the SHUN FA's registered IMO number, almost no maritime observers could reasonably be expected to recognize it as the KINGSWAY.

In this way, the KINGSWAY successfully skirted the consequences of its designation and operated at will for nearly three years—until its detention in Busan, South Korea in May 2021.⁴⁴

Case Study

TYPE 2 INDIRECT VESSEL IDENTITY LAUNDERING: THE SUBBLIC

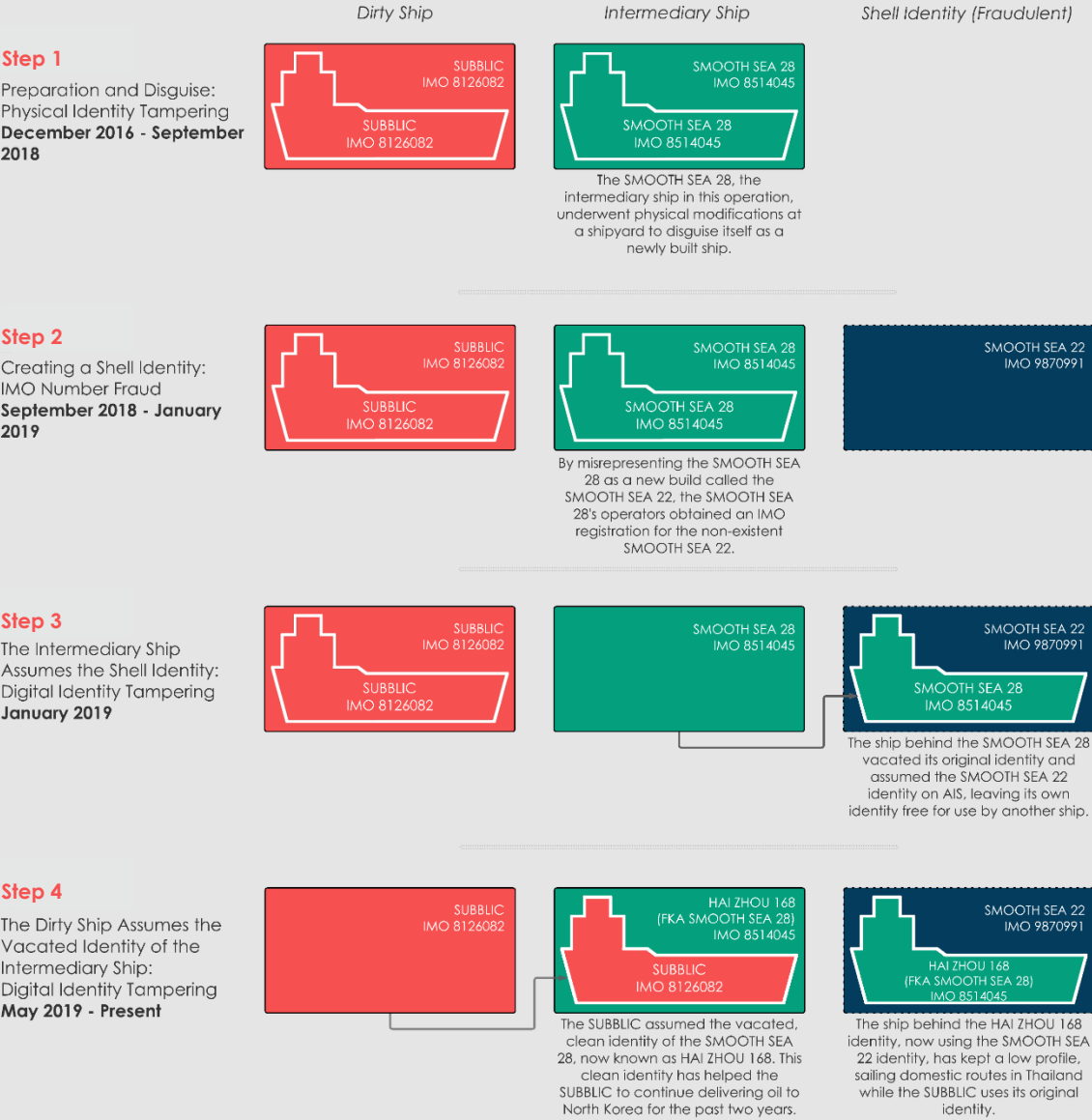
The SUBBLIC (IMO 8126082) is a familiar name for DPRK sanctions monitors. A regular in the UN Panel of Experts reports and maritime advisories, the SUBBLIC has reportedly delivered oil to North Korea at least 17 times in 2019 and 2020, and has been recommended for designation multiple times.⁴⁵

The SUBBLIC has not transmitted AIS from its own identity since February 2018. Yet satellite imagery confirms that the SUBBLIC is an active ship that regularly travels to North Korea, including as recently as June 2021.




In this case study, we see that the SUBBLIC has been able to operate freely by undergoing a Type 2 indirect vessel identity laundering operation to assume a “clean” identity—the HAI ZHOU 168 (IMO 8514045)—after the genuine HAI ZHOU 168 vacated its digital identity and assumed a shell identity.⁴⁶

SUBBLIC Vessel Identity Laundering Operation

Indirect Vessel Identity Laundering Operation into the HAI ZHOU 168




LEGEND



Rectangular boxes represent an independent registered identity of a ship. A solid box denotes a legitimately registered identity, while a dotted line denotes a fraudulent registration (i.e. a shell identity).

The ship icon represents the actual vessel behind a registered identity. As there is no real vessel associated with a shell identity, shell identities do not have a ship inside of them.



The arrow represents the movement of a ship as it vacates one identity and assumes another.

Step 1 Preparation and Disguise: Physical Identity Tampering

In February 2018, a surveillance aircraft photographed the SUBBLIC (then known as the XIN YUAN 18) engaging in a ship-to-ship (STS) transfer with a North Korean oil tanker.⁴⁷ After images of the SUBBLIC's illicit STS transfer were published in the media, the SUBBLIC was burnt. Continuing to use this identity would subject the ship and its associated entities to scrutiny from international sanctions monitors and secondary sanctions risk. As a result, the SUBBLIC never transmitted under its own registered identity again to date.



Surveillance photos of the XIN YUAN 18 (nka SUBBLIC) captured by the Japanese military. Source: Japan Ministry of Defense.⁴⁸

However, more elaborate plans were in motion elsewhere to provide the SUBBLIC with a way to continue to deliver oil to North Korea. The first phase of an identity laundering operation was underway using an intermediary ship: the SMOOTH SEA 28 (IMO 8514045). The SMOOTH SEA 28, an old Thailand-flagged oil tanker, first moored at a dock in Bangkok in December 2016. Over the next 20 months, satellite imagery and social media photos show that the vessel underwent a complete reconstruction of its deck. When these modifications were finally complete in September 2018, the SMOOTH SEA 28 looked completely different.

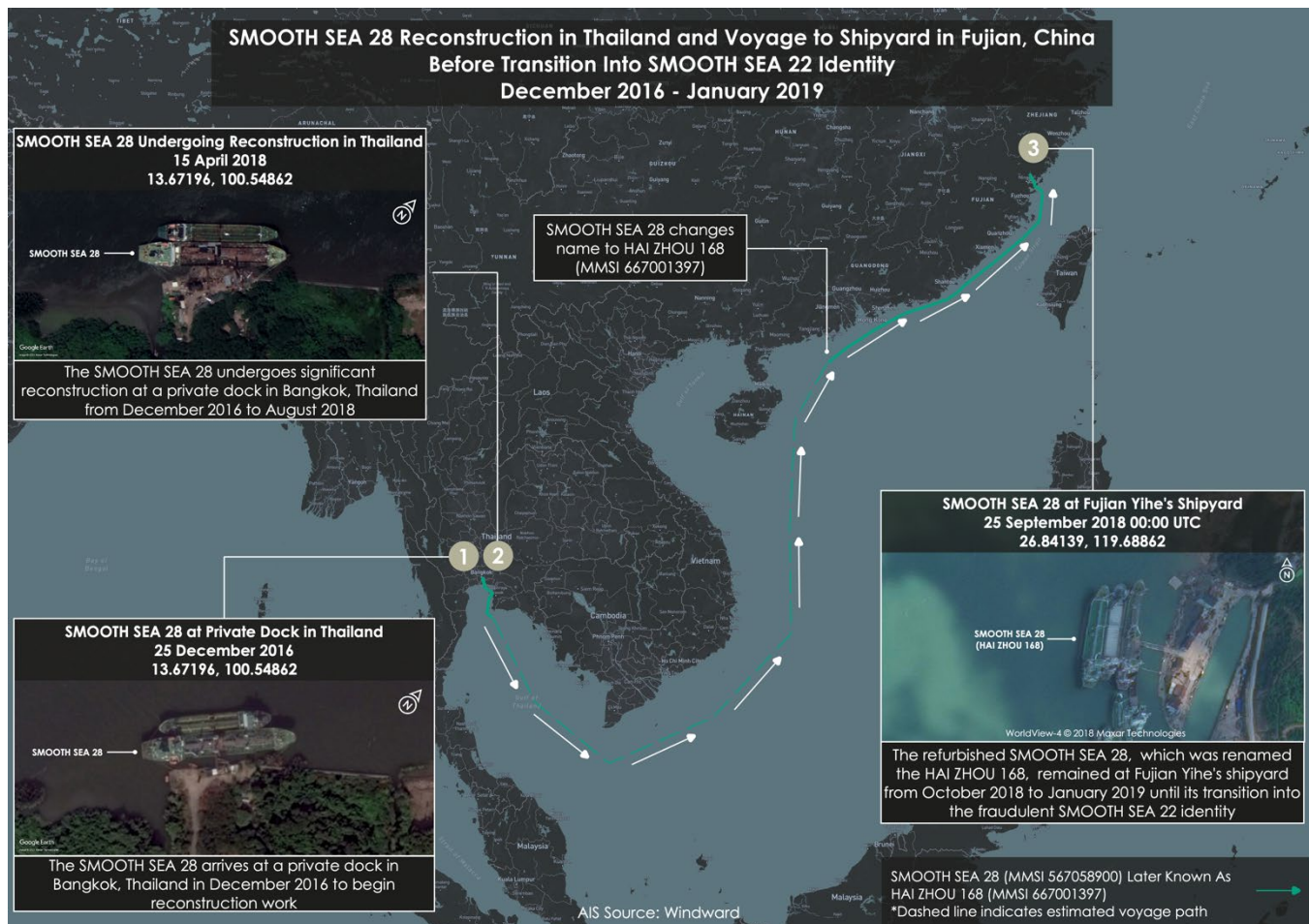


Left: Photo of the SMOOTH SEA 28's original deck likely uploaded by a crewmember in June 2015. Middle and Right: Photos of the SMOOTH SEA 28's reconstructed deck possibly uploaded by a contractor in August 2018. Source: Facebook.

With this new physical identity, the SMOOTH SEA 28 departed Bangkok and sailed to China.

Step 2 Creating a Shell Identity: IMO Number Fraud

On 22 September 2018, the SMOOTH SEA 28 arrived at a shipyard owned by Fujian Yihe Shipbuilding Industry Co., Ltd. (福建省易和船舶重工有限责任公司; “Fujian Yihe”) located on the banks of the Jiaoxi Brook in Ningde, Fujian Province, China.⁴⁹



After a nearly two-year reconstruction of the SMOOTH SEA 28 in Thailand, the vessel sailed to a shipyard in China where it prepared to transition into the fraudulent SMOOTH SEA 22 identity, a supposedly newly built vessel. Source: Imagery provided by Google Earth and Maxar Technologies; AIS data provided by Windward.

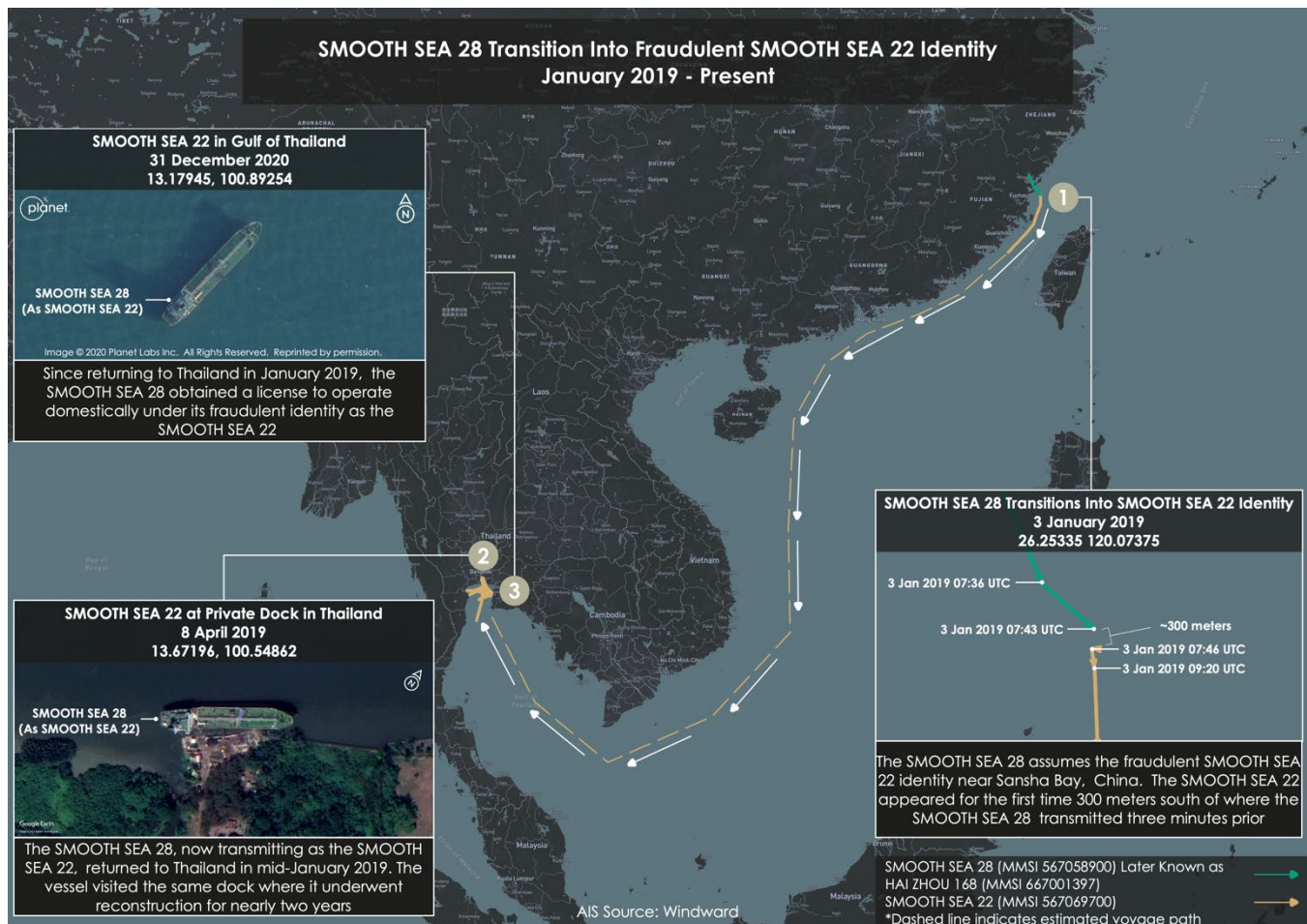
Four days after the SMOOTH SEA 28's arrival, maritime records indicate that Fujian Yihe supposedly launched a newly built oil tanker: the SMOOTH SEA 22 (IMO 9870991).^{50 51} On paper, the SMOOTH SEA 22 and SMOOTH SEA 28 share similar physical dimensions and mechanical details.⁵²

But there was no new ship. Instead, the SMOOTH SEA 22 was likely a shell identity created for the SMOOTH SEA 28, which now looked like a newbuild ship after being reconstructed in Thailand over the past two years. With the SMOOTH SEA 28 positioned in Fujian Yihe, the ship's operators

likely also used fraudulent documents to help present it as the SMOOTH SEA 22 in order to obtain the new IMO number 9870991.

Step 3 The Intermediary Ship Assumes the Shell Identity: Digital Identity Tampering

The SMOOTH SEA 28 was now ready to assume the shell identity of the SMOOTH SEA 22. On 2 January 2019, the SMOOTH SEA 28, which had been regularly transmitting AIS while moored at Fujian Yihe's shipyard, sailed out of the Jiaoxi Brook into Sansha Bay, where its AIS signal disappeared. Three minutes later, the SMOOTH SEA 22 broadcast AIS transmission for the first time, approximately 300 meters from where the SMOOTH SEA 28's AIS signal had disappeared minutes earlier. At this point, the SMOOTH SEA 28 appears to have vacated its registered identity and assumed the shell identity of the SMOOTH SEA 22.



After assuming the fraudulent SMOOTH SEA 22 identity in January 2019, the vessel originally registered as the SMOOTH SEA 28 returned to Thailand. Source: Imagery provided by Planet Labs, Google Earth, and Maxar Technologies; AIS data provided by Windward.

Step 4 The Dirty Ship Assumes the Vacated Identity of the Intermediary Ship: Digital Identity Tampering

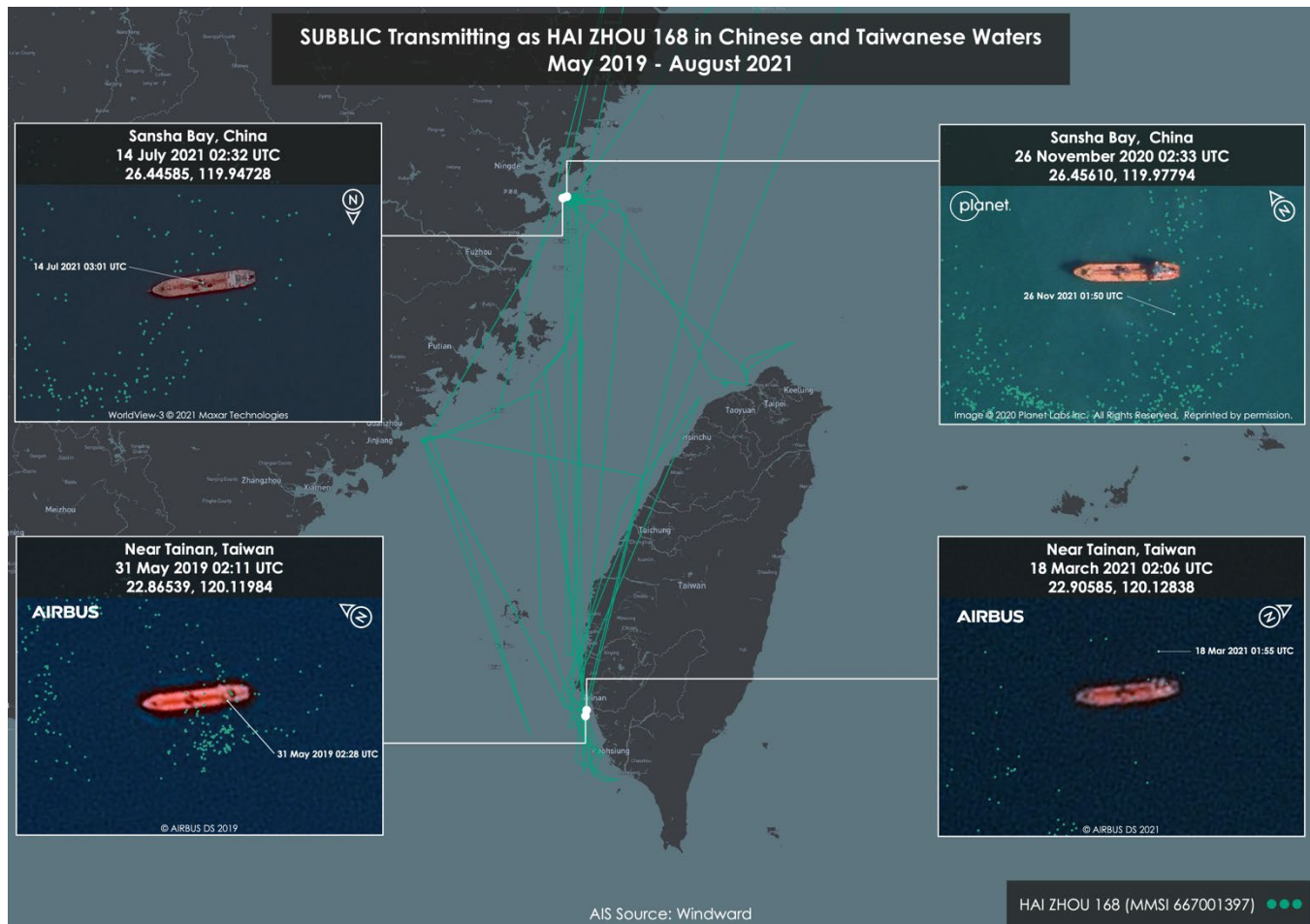
With the SMOOTH SEA 28 now having likely adopted a new shell identity, the next phase of the vessel identity laundering operation was ready to begin.

After assuming the identity of the SMOOTH SEA 22 in January 2019, the SMOOTH SEA 28's registered identity was left vacant. This does not appear to be an accident. Two months later, ownership and management of the SMOOTH SEA 28, which was now renamed the HAI ZHOU 168 in maritime records, were transferred to a company named Milyan R Trade International Co. Ltd. (邁源紅貿易國際有限公司; "Milyan R").^{53 54}

It is important to note that this transfer occurred after the HAI ZHOU 168 had vacated its original identity. No company would be willing to buy a nonexistent ship. This suggests that the HAI ZHOU 168's new operators were aware that the identity was vacant. In other words, Milyan R was not buying a physical vessel in March 2019 when they assumed ownership of the HAI ZHOU 168. What they were (likely wittingly) buying was a fully registered vacant identity for another vessel to use.

Here is where the SUBBLIC comes back into the picture. The only other ship managed and owned by Milyan R at this time was the SUBBLIC. With all of the negative attention that the vessel had received following its transfer of oil to North Korean interests, the operators of the SUBBLIC had an incentive to obtain a new, clean identity for the ship.

The newly acquired HAI ZHOU 168 identity fit the bill—unassociated with any derogatory information, and free from the risk of parallel transmission by the original ship which was using the SMOOTH SEA 22's identity. In March 2019, the HAI ZHOU 168 started transmitting AIS again, two months after its identity was vacated. Satellite imagery captured in May 2019 revealed that the vessel that had assumed the identity of the HAI ZHOU 168 was the SUBBLIC, whose whereabouts had been unknown since February 2018. The imagery showed that the SUBBLIC's deck had been repainted orange, possibly in an attempt to enhance its disguise after assuming the HAI ZHOU 168's identity.



Satellite imagery shows the SUBBLIC has used the vacated HAI ZHOU 168 identity from 2019 to the present. Source: Imagery provided by Planet Labs, Airbus Defence and Space, and Maxar Technologies; AIS data provided by Windward.

Over the next two years, the SUBBLIC would use the HAI ZHOU 168's identity while anchored in Chinese and Taiwanese territorial waters and while sailing to and from North Korea. Assuming a clean registered identity enabled the vessel to transmit AIS freely in Taiwanese waters, a hotspot for at-sea oil transfers, without risk of detection or detainment.⁵⁵ Transactions involving the SUBBLIC could be arranged without risk of failing a due diligence check. Further, the SUBBLIC's partners, and even maritime regulators, whether aware or not of the vessel identity laundering operation, had plausible deniability if the SUBBLIC's cover were to be blown.

THE USE OF THE HAI ZHOU 168 IDENTITY BY OTHER “DIRTY” SHIPS

The SUBBLIC is not the only DPRK-linked vessel to have transmitted the HAI ZHOU 168 identity. Although the SUBBLIC is the primary user of the HAI ZHOU 168 identity, the XING MING YANG 888 (IMO 8410847), another foreign-flagged oil tanker identified by the UN Panel of Experts for conducting direct deliveries and STS transfers of fuel to North Korea, has been observed in

satellite imagery and AIS data transmitting the HAI ZHOU 168 identity while anchored in Taiwanese waters in May 2020.⁵⁶ When the HAI ZHOU 168 identity is occupied by another vessel, the SUBBLIC has adopted other interim fraudulent vessel identities.



Satellite imagery shows another DPRK-linked tanker, the XING MING YANG 888, used the HAI ZHOU 168 identity while anchored near Kaohsiung Port, Taiwan in May 2020. Source: Imagery provided by Airbus Defence and Space; AIS data provided by Windward.

The use of the HAI ZHOU 168 identity by other DPRK-linked vessels indicates likely coordination between the networks of these dirty ships. In order to maintain the ruse, the vessels sharing a clean, vacated identity must ensure that the “hand-off” from one vessel to another does not arouse suspicion. If the vessels simultaneously transmit the same identity on AIS or exhibit anomalous voyage patterns while using the clean identity, the risk of exposure increases. However, if the transition is executed correctly, this provides multiple networks with a transferrable sanctions evasion capability that presents further challenges for sanctions monitors.

KEY TAKEAWAYS

The cases of the KINGSWAY and SUBBLIC highlight the numerous loopholes and vulnerabilities in the maritime industry that allow ships to misrepresent their registered, digital, and physical identities. In this section, we explore the lessons learned from known vessel identity laundering operations, as well as possible solutions to address weaknesses in the international regulatory system.

IMO NUMBER FRAUD: CREATING A SHELL IDENTITY

The shipping industry has long been criticized for its regulatory loopholes and poor governance. For many years, maritime experts have pointed out vulnerabilities in shipping practices, such as the widespread use of flags of convenience, AIS tampering or manual switch off, and the use of shell companies to conceal beneficial ownership. These tactics have been rife among vessels evading sanctions or conducting illicit trade. Many of these problems arise from the inability of the IMO, a multilateral organization represented by stakeholders with competing interests, to reach a consensus on regulation and enforce standards across the industry.

However, vessel identity laundering operations present a new and unexpected challenge; they strike at the IMO's cataloguing and management of the global fleet, a system that *all* maritime stakeholders are dependent on for accurate record-keeping and identification of ships worldwide. The international shipping order has operated on the basis that an IMO number is an authoritative and unique identifier issued to one ship—a real ship, if that has ever needed to be spelled out. What we see in the cases of the KINGSWAY and SUBBLIC is how the IMO registration process can be hijacked to issue a registered identity and IMO number to a non-existent vessel, which in turn can be used to disguise the identity of other IMO-registered ships. It challenges the notion that maritime stakeholders can use at least one of the three facets of a ship's identity—registered, digital, and physical—to know that a ship is who it claims to be.

Vessel identity laundering threatens the integrity of the international sanctions regime, which relies on a vessel's IMO number to identify and blacklist offenders. However, the overall impact of this typology is much larger than how ships can avoid sanctions enforcement, as it introduces identity fraud of an unprecedented extent to the shipping ecosystem. What if a non-existent ship is used as collateral in a loan? What if a ship is a newbuild according to its registered identity, but the actual ship sailing under that identity is a decades old rust bucket with serious safety hazards? Who is liable, and who is vulnerable? Can industry stakeholders protect themselves against this type of deception?

These case studies demonstrate real challenges to the IMO's due diligence protocols. In these examples, we see that the IMO was not able to confirm that:

1. The vessel applying for an IMO number is a real ship;
2. It has never been issued an IMO registration in the past; and
3. The vessel details and documents submitted in the application are true and legitimate.

In the case of the SUBBLIC's identity laundering, the SMOOTH SEA 28 underwent extensive physical modifications to disguise the ship, which was actually built in 1986, as a new construction. While the extensive alterations to the vessel's physical features admittedly complicates the detection of the so-called SMOOTH SEA 22 as an existing vessel, the IMO was unable to discern that this newbuild was in fact, an old vessel that had been active for over 30 years, and that therefore, there was no real vessel to register. An in-person vessel inspection, for example, would immediately reveal signs that the ship was an aged build.

As the details of a ship's registration and its supporting documents are not publicly available, the authors are not aware of the precise nature of this deception—whether documents were forged, and if so, how and to what degree. Nonetheless, legitimizing the existence of the SMOOTH SEA 22 and claiming it as a newbuild likely required false documents testifying as such, and this fraud went undetected by the IMO.

In a nutshell, the IMO should realize the IMO registration system's full potential as a tool for regulation. Its due diligence procedures should match the authority that the international shipping industry confers onto the IMO number system. The authors acknowledge that it is not an easy feat to see a photo of a ship that is under disguise and to immediately recognize it for its true identity. This requires not only the knowledge that the vessel is misrepresenting its identity, but the ability to find photographs of the registered ship that the vessel is in actuality among tens of thousands of others. To conduct this type of check in every vessel registration is admittedly a high due diligence and investigative burden, and it is unrealistic to expect dramatic changes to happen overnight. However, IMO's requirements in a ship's registration application can be tightened in several ways that are significantly lower lifts.

Firstly, the IMO should require resubmission of vessel photographs and current information from operators at regular intervals for ships to maintain their registration, and deregister ships that do not comply. The IMO's current vessel registration system largely relies on ship operators to self-report changes to their status (e.g. when a ship undergoes a name change). As a result, changes to a ship's identifiers, such as its flag registration or current status, are not conveyed to the IMO and reflected on the IMO's records in a timely manner. Sometimes, these details are not reported at all, and there are ships in the IMO's system who have reported zero updates over suspiciously long periods of time. While this may not be a red flag in and of itself, it is likely that records for these vessels are outdated, meaning that their identities may be more liable to exploitation by illicit actors. This can be mitigated by mandating operators of IMO-registered ships to report vessel details and submit photographs of the ship to the IMO at regular intervals in order to retain the vessel's registration. Similarly to how people are required to apply for a new passport every few years to ensure that the identifying information on that document is current and the photograph is a genuine representation of the person, the IMO should require ship operators keep records on their vessels updated and accurate.

Secondly, the IMO should require ship owners and operators to submit a complete set of identifying information and specifications for their ships when applying to register. IMO records on registered ships often contain missing data fields. A particularly common set of missing data is a ship's recorded dimensions. Despite registration application documents having fields to capture this data, it appears that applicants are not penalized for not providing information for all fields. This resultantly makes identification of ships harder, as there are fewer data points to reference in the IMO's records on the vessel. In particular, the lack of official data on dimensions

complicates investigation of vessel identity tampering or laundering for regulators, who frequently use the length and breadth of ships to identify ships in imagery. Similarly, mandating the submission of identifiers that are hard to tamper with—such as a ship's hull or engine number—would provide regulators with another reference point to verify a ship's identity, as well as to increase the costs of physical identity tampering in vessel identity laundering operations. Therefore, the IMO should mandate vessel owners and operators to fill out all requested data fields, and publish these details in public records (such as GISIS), so that all maritime stakeholders have access to a greater range of information on registered ships.

Similarly, the IMO should require each registration application to submit photographs of ships from key angles, to include images of the ship on all four sides, as well as superstructures on its deck. These photographs should be used to assess the veracity of a ship's application, and also included in a ship's records on GISIS to ensure all maritime stakeholders can check these images as needed. In particular, these photographs will serve as a credible reference point for regulators when comparing known pictures of ships against satellite or ground level imagery in which a ship is unidentified, or its identity is in doubt.

If implemented, these improvements to the IMO's registration system would meaningfully challenge the ability of illicit actors to commit IMO number fraud and create shell identities on demand, as well as to increase the costs associated with such attempts. These due diligence enhancements will better allow the IMO to regulate shipping practices and ensure the integrity of the global fleet's registered identities.

AIS MANIPULATION: TAMPERING WITH A SHIP'S DIGITAL IDENTITY

Vessel identity laundering, in addition to requiring the creation of at least one fraudulent IMO-registered identity, involves vessels manipulating their AIS transmissions to transmit under the identifiers of another ship. This type of AIS manipulation or tampering is a long-recognized problem in the maritime domain, to which a solution is long overdue.

Ensuring AIS Transponder Standards

While all stakeholders in the shipping space operate with the notion that AIS is key to safe navigation at sea and must not be tampered with in any way, including switching off AIS transmissions or broadcasting false data, the reality is that AIS transponders simply are not constructed to be fully tamper proof, and bad actors take advantage of this fact.

Although the process of obtaining a MMSI number is heavily regulated, it is not so for the AIS transponder which transmits the MMSI number. AIS transponders can be purchased from manufacturers, dealers, or the secondhand market just like any other consumer electronic device. There are dozens of transponder models from various manufacturers, each of which may have different security measures to prevent AIS tampering. For example, some transponders only allow the user to enter the ship's identifying information such as the MMSI number once; any subsequent changes require, at least theoretically, some form of support from the manufacturer or an authorized technician. Other transponders are delivered to the

user with the MMSI number pre-configured. Regardless, although industry has implemented some security measures for AIS transponders, they are inconsistent and insufficient.

Regulators and industry should come together to develop—and update regularly—a set of hardware, software, and product servicing standards that specifically targets the threat of AIS tampering. Transponder models and manufacturers that attain these standards receive a special certification, which can help flag registries, governments, financial institutions, and other maritime stakeholders identify the most secure equipment for use by ships under their jurisdiction. Shipowners that do not use a certified transponder can be denied services, subjected to increased monitoring, or otherwise penalized. Securing the AIS transponder is key to preventing vessel identity laundering, as well as many other typologies of identity tampering and obfuscation practiced by ships conducting illicit activities. This will be discussed in further detail in the recommendations section of this report.

Tracking AIS Tampering

Despite the widespread problem of AIS-based identity manipulation and ships turning off their AIS signal while participating in high-risk activities, maritime regulators often lack the means or are not motivated to detect and prevent AIS tampering.

Ensuring correct and consistent broadcasting of AIS is a responsibility that falls primarily onto flag registries, who are tasked with enforcing international maritime regulations over their registered fleet. They are the first line of defense against AIS tampering behavior. Some, however, are simply not willing to invest the resources and time required to maintain visibility over the AIS transmissions of their registered ships. Many AIS tracking or maritime intelligence platforms are not free, and even in cases where flag registries make use of these solutions, detecting and confirming that a vessel is tampering with its AIS data requires investigative effort. For registries that are often classified as providing flags of convenience, and see vessel registration as a source of revenue rather than a utility that the government provides for the registration of vessels with tangible links to the state, investing further resources to raise its regulatory standards not only cuts into their bottom line, but also renders them less attractive to vessel operators seeking low regulation environments. Moreover, the IMO can create resolutions to put forward best practices and standards, but there are no mechanisms for the IMO to compel states, or penalize those that fall short. In sum, the IMO lacks both carrots and sticks to enforce AIS operation standards worldwide, leaving loopholes open to exploitation by illicit actors.

To complicate matters further, vessel identity laundering is hard to detect through AIS transmissions only. Previously observed instances of vessel identity tampering, e.g. using another vessel's IMO number or MMSI number without the counterpart's awareness, often leaves traces, such as parallel transmissions or “fusion jumps” as the vessel assuming a fraudulent identity transmits AIS at a location far from the location of the vessel it has assumed the identity of. In comparison, vessel identity laundering is significantly more sophisticated and coordinated. All ships and parties involved in the operation move in sync; vessels schedule the vacating and occupying of digital identities to prevent simultaneous transmissions under the same identity. This makes discovering cases of vessel identity laundering over AIS extremely challenging without combining it with other data, such as satellite imagery to “see” what is physically happening.

Nonetheless, flag registries and other maritime regulators need to be aware of vessel identity laundering tactics, and monitoring and reporting AIS anomalies and discrepancies, as it is impossible to understand vessel identity laundering without AIS visibility. Plus, in some cases, vessel identity laundering can leave digital breadcrumbs. For example, when the KINGSWAY and TWINS BULL swapped their fraudulent profiles of the ALPHA and UNI WEALTH while moored in Keelung, the operators made the error of transmitting the same IMO number between both fraudulent identities. In no legitimate circumstance would ships broadcast the same IMO number; at least one of those ships would be making a fraudulent transmission. This was a giveaway that regulators, such as the Mongolian flag registry (with which both fraudulent identities were registered), or the port authority in Keelung, should be able to flag and investigate.

In sum, recognizing and preventing AIS tampering, especially in stopping identity laundering operations requires participation by all maritime regulators. On the one hand, it is about empowering regulators through resources, data-sharing, and capacity building; on the other, it is about holding maritime regulators across the globe to account. Other maritime stakeholders too, such as banks and insurance companies, should strengthen their AIS tracking capabilities and maritime domain awareness to protect themselves against vessels misrepresenting their true identities through AIS manipulation.

MODIFICATIONS AND FALSE NEW BUILDS: TAMPERING WITH A SHIP'S PHYSICAL IDENTITY

Ships undergo repainting or structural reform and repair for many legitimate reasons, and these physical modifications are not in and of themselves indicative of identity tampering, laundering, or participation in illicit activity. However, in vessel identity laundering operations, ships undergo a critical physical alteration that is in contravention of international law. 2002 amendments to SOLAS Regulation XI-1/3 mandates ship identification numbers to be permanently marked on the ship's hull or superstructure, in a clearly visible area.⁵⁷ Therefore, when ships in vessel identity laundering schemes paint over their original IMO numbers, and paint a different IMO number and name to present itself as that new identity, this is a breach of international maritime law.

As this act of misrepresenting a ship's IMO number is illegal, the parties involved in painting IMO numbers different to the ship's original are wittingly participating in a criminal act. Whether the responsible parties may be shipyards involved in a ship's modification, or crew onboard a vessel, they are facilitators of vessel identity laundering and abetting crime.

Shipyards, in particular, pose a large threat to the integrity of a vessel's physical identity. Without going to a shipyard, the types of physical alterations that ships can undergo are limited. As we saw in the case of the SMOOTH SEA 28 and the creation of the false SMOOTH SEA 22 profile, the shipyard in Thailand made significant modifications to the SMOOTH SEA 28's deck and superstructure. While making changes to ship's structure can be argued as justifiable under a number of reasons (e.g. repairs, repurposing of a vessel, etc.), it is highly likely that in this case, the modifications were for the purpose of changing the appearance of the SMOOTH SEA 28 in preparation to disguise it as a new build and obtain a shell identity. Presumably in doing this, the shipyard purposefully obscured the SMOOTH SEA 28's original IMO number painting, and issued

false documents that presented the so-called SMOOTH SEA 22 as a newly-constructed ship. These acts are intentional and designed to mislead maritime regulators. They are also defrauding other stakeholders in the shipping industry, such as banks, who may issue mortgages with these ships as collateral, or insurance companies. Redecorating a 30-year old house and posing it as a new building in a mortgage application is illegal and presents risks to the lender; the case with these ships is no different.

Naturally, these facilitators should be duly held responsible. However, the novelty and complexity of vessel identity laundering operations have complicated resolution and the creation of new regulation to mitigate these vulnerabilities. In the meantime, entities that have been identified as facilitating vessel identity laundering operations should be carefully monitored to prevent future cases of physical identity tampering.

RECOMMENDATIONS

In light of this report's findings, the authors suggest the following recommendations for the maritime community and its regulators.

REGISTERED IDENTITY

IMO number fraud and loopholes in the IMO's registration system enable vessel identity laundering operations. As the most authoritative regulatory organ in shipping, the IMO must implement stricter regulatory standards and due diligence checks in the registration and operation of the global shipping fleet.

- The IMO should require resubmission of vessel photographs and current details from operators at regular intervals for ships to maintain their registration, and deregister non-compliant vessels.
 - The IMO should publish a list of vessels that are purged from the global fleet, to ensure that it is broadly known that those vessels are no longer IMO-registered, and illicit actors cannot exploit their identities.
- The IMO should publish a list of IMO numbers that are cancelled and vessels whose registrations are rescinded.
- The IMO's Maritime Safety Committee should coordinate a working group of representatives from government, industry, and civil society organizations to strengthen risk screening procedures for the IMO number application process.
 - Require IMO number applications to be filled out in the entirety, and include compulsory fields such as hull number and engine number.
 - Mandate submission of photos in applications.
 - Create a spot check procedure to detect fraudulent documents
 - Authenticate certificates issued by flag registries and classification societies by getting confirmation from these authorities.
- The IMO's Maritime Safety Committee should promote transparency of the IMO number system by publishing annual reports that outline the measures taken to combat IMO number fraud, statistics on registration trends, case studies, and other guidance on evasion typologies.

DIGITAL IDENTITY

AIS tampering is an increasingly widespread tactic used to obfuscate the activity and identity of ships that participate in illicit activities, and is a critical enabling step in vessel identity laundering operations. Enforcing standards on AIS transponders to prevent false inputs and improving AIS monitoring across all maritime stakeholders is essential to eradicating this practice.

- The IMO's Maritime Safety Committee should coordinate a working group of representatives from government, industry, and civil society organizations to develop hardware and software security standards for preventing the tampering of AIS transponders. This working group should produce a list of AIS transponder models that meet anti-tampering standards for both Class A and Class B transponders. The transponder model's certification should be reviewed regularly.
 - Transponders should not be reprogrammable onboard and have better tamperproof measures than having manual reset codes built in for backend access.
 - The IMO should consider creating a global registry for AIS transponders and issue each transponder with a unique identifier, which is included in the transponder's AIS transmissions. This will provide more clarity in maritime records of which vessels are using which transponders, as well as each IMO number/MMSI number that has historically been entered into a transponder.
 - The International Telecommunications Union (ITU) should ensure that Member States are regularly submitting lists of registered ship stations and their MMSI numbers to the Maritime Mobile Access and Retrieval System (MARS). The ITU should publish annual reports on the registration trends and compliance from Member States.
- Flag registries and other maritime authorities should implement tools and methods to detect AIS tampering or anomalies by ships under their jurisdiction, and information on detected cases should be published and shared with other maritime regulators.

PHYSICAL IDENTITY

In vessel identity laundering operations, ships modify their physical appearance to deliberately misrepresent their identities and deceive regulators. Presenting a false IMO number is in breach of international maritime law.

- All maritime regulators and enforcement agencies should detain and investigate ships that have painted over their original IMO number and marked a different one, as well as any other entities responsible for facilitating identity tampering.

INCREASED DATA SHARING AND COMMUNICATION

In shipping, a variety of stakeholders each hold different information on a ship's identity and activities. Ensuring that this information is shared among all relevant parties is key to preventing illicit actors from exploiting data gaps and loopholes in the maritime domain.

- The IMO should mandate the expansion of ship information provided in GISIS to include the following data points:
 - Vessel specifications (e.g. length, breadth, gross tonnage, deadweight tonnage)
 - Historical MMSI numbers and call signs, complete with periods of use
 - Photographs submitted to the IMO
- The IMO should mandate the GISIS to distinguish whether a vessel's flag registration is provisional or permanent. If a vessel's flag registration is provisional, GISIS should indicate the date of issue and expiry. GISIS should prominently mark the vessels whose provisional flag registration status has expired.
- The IMO should create a secure communication channel where the public and whistleblowers can submit information on vessels, individuals, companies, and officials that are abusing or facilitating the abuse of the IMO number system.
- The UN Panel of Experts on the DPRK should include in its midterm and final reports a table of fraudulent IMO-registered and AIS identities used by vessels linked to DPRK sanctions evasion activities.
- Governments should regularly publish circulars and advisories that include lists of fraudulent IMO-registered and AIS identities used by DPRK-linked vessels. Governments should ensure that these blacklists are disseminated to authorities responsible for maritime security.

INDUSTRY-WIDE BEST PRACTICES AND OTHER RECOMMENDATIONS

Preventing ships from engaging in vessel identity laundering as well as any other obfuscation practices requires a whole-of-society response, including international and national-level regulators, law enforcement, and private industry.

- Governments and law enforcement (at the national and international levels) should investigate vessel identity laundering networks for potential ties to organized crime and other illicit activities or maritime practices.
- Governments should expand the definition of sanctions facilitation to include helping sanctioned entities or entities engaging in sanctionable activities to evade authorities, such as by tampering with a ship's identity. Entities that play key roles in vessel identity laundering operations such as shipyards should be held accountable.
- Flag registries should end the practice of recycling MMSI numbers and call signs.

- Commercial maritime intelligence platforms should distinguish between vessels broadcasting from a Class A or B AIS transponder and allow users to filter for either transmission type.⁵⁸
- Commercial maritime intelligence platforms should clarify which data points in a vessel's profile came from AIS and third-party providers.

END NOTES

¹ N/A. (n.d.). AIS Transponders. International Maritime Organization.

<https://www.imo.org/en/OurWork/Safety/Pages/AIS.aspx>.

² N/A. (n.d.). IHS Markit Maritime Intelligence Risk Suite (MIRS). IHS Markit. <https://mirs.maritime.ihs.com>.

³ N/A. (2006, October 14). Resolution 1718: Non-proliferation/Democratic People's Republic of Korea. United Nations Security Council. <http://unscr.com/en/resolutions/doc/1718>.

⁴ N/A. (n.d.). IHS Markit Maritime Intelligence Risk Suite (MIRS). IHS Markit. <https://mirs.maritime.ihs.com>.

⁵ K, R. (2021, April 16). What is IMO's Global Integrated Shipping Information System (GISIS)? Marine Insight. <https://www.marineinsight.com/maritime-law/what-is-imos-global-integrated-shipping-information-system-gisis/>.

⁶ N/A. (n.d.). Introduction to IMO. International Maritime Organization. <https://www.imo.org/en/About/Pages/Default.aspx>.

⁷ Kantharia, R. (2020, December 22). What is International Maritime Organization (IMO)? Marine Insight. <https://www.marineinsight.com/maritime-law/what-is-international-maritime-organization-imo/>.

⁸ N/A. (n.d.). IHS Markit Maritime Intelligence Risk Suite (MIRS). IHS Markit. <https://mirs.maritime.ihs.com>.

⁹ N/A. (2021, August 17). Maritime Mobile Service Identity. U.S. Department of Homeland Security Navigation Center. <https://www.navcen.uscg.gov/?pageName=mtmmsi>.

¹⁰ Wankhede, A. (2021, August 16). What is Ship-to-Ship transfer (STS) and Requirements to Carry Out the Same? Marine Insight. <https://www.marineinsight.com/maritime-law/what-is-ship-to-ship-transfer-sts-and-requirements-to-carry-out-the-same/>.

¹¹ N/A. (n.d.). SOLAS. International Maritime Organization: Knowledge Center. <https://www.imo.org/en/KnowledgeCentre/ConferencesMeetings/Pages/SOLAS.aspx>.

¹² N/A. (n.d.). Work and Mandate. United Nations Security Council. https://www.un.org/securitycouncil/sanctions/1718/panel_experts/work_mandate.

¹³ N/A. (n.d.). IMO Identification Number Schemes. International Maritime Organization. <https://www.imo.org/en/OurWork/IIS/Pages/IMO-Identification-Number-Schemes.aspx>.

¹⁴ N/A. (n.d.). IMO Ship and Company Number Scheme. IHS Markit. <https://ihsmarkit.com/products/imo-ship-company.html>.

¹⁵ N/A. (n.d.). IMO Ship and Company Number Scheme. IHS Markit. <https://ihsmarkit.com/products/imo-ship-company.html>.

¹⁶ N/A. (2020, November 23). AIS Frequently Asked Questions. U.S. Department of Homeland Security Navigation Center. <https://www.navcen.uscg.gov/?pageName=AISFAQ>.

¹⁷ N/A. (n.d.). SOLAS Chapter V, Regulation 19.2. U.S. Department of Homeland Security Navigation Center. <https://www.navcen.uscg.gov/pdf/AIS/SOLAS.V.19.2.1-5.pdf>.

¹⁸ MMSI numbers are issued by administrations/geographical areas and regulated by the International Telecommunications Union (ITU), a UN specialized agency. In order to obtain a MMSI number for a vessel, the user must apply to the relevant government agency (e.g. the Federal Communications Commission in the US) or a third-party entity (e.g. company authorized by the administrator). Once the MMSI number and associated ship radio station license are granted, the MMSI number can be entered into the vessel's AIS transponder. Unlike an IMO number, a vessel's assigned MMSI number can change as the vessel changes flags and ownership. Although some administrators do recycle MMSI numbers formerly assigned to ships that have exited their jurisdiction, a MMSI number should only be issued to and used by one ship at a time. Sources: N/A. (2021, August 17). Maritime Mobile Service Identity. U.S. Department of Homeland Security Navigation Center.

<https://www.navcen.uscg.gov/?pageName=mtmmsi>; N/A. (2014, October 1). ITU-BR Guidance for Administrations on Maritime Radiocommunications. International Telecommunication Union. <https://www.itu.int/en/ITU-D/Regional-Presence/AsiaPacific/Documents/Events/2018/PRW-18/Presentations/ITU%20guidance.pdf>.

¹⁹ N/A. (2021, August 17). Maritime Mobile Service Identity. U.S. Department of Homeland Security Navigation Center. <https://www.navcen.uscg.gov/?pageName=mtmmsi>.

²⁰ There are two main types, or classes, of AIS transponders: Class A and Class B. Both classes transmit a vessel's static and dynamic information, but Class A transponders have additional functions required by the IMO that enable the vessel to conform to international maritime protocols and operate safely on the high seas. Class B transponders are not fully compliant with IMO requirements but confer the navigational benefits of AIS to users at a

lower cost. Due to their technical configurations, Class B transponders typically have lower range and transmit with less frequency than Class A transponders. Notably, Class A AIS messages can include the vessel's IMO number; Class B AIS messages do not. A list of the AIS messages that can be transmitted by each transponder class can be found here: <https://www.navcen.uscg.gov/?pageName=AISMessages>. Source: N/A. (2020, December 3). Types of Automatic Identification Systems. U.S. Department of Homeland Security Navigation Center.

<https://www.navcen.uscg.gov/?pageName=typesAIS>.

²¹ Makleff, M. (2020, January 8). True Identity. Windward. <https://windward.ai/blog/true-identity/>.

²² Due to the sensitive nature of the information shared in these forums, the authors have withheld the sources.

²³ Li, X. (2022, November 22). "One Ship, Two Codes" Maritime Safety Administration of Yichang Village, Guizhou City Calls for Urgent Stop! (translated) soship.com. <https://news.soship.com/show/194810/>.

²⁴ N/A. (2020, August 27). Jiangsu Strictly Investigated "One Ship Multiple Codes" and Began Implementing Punishments (translated). cssglw.com. <https://www.cssglw.com/news/200827134606243916.html>.

²⁵ N/A. (2019, March 5). S/2019/171. United Nations Security Council. <https://undocs.org/S/2019/171>.

²⁶ N/A. (2018, March 5). S/2018/171. United Nations Security Council. <https://www.undocs.org/S/2018/171>.

²⁷ N/A. (2019, March 5). S/2019/171. United Nations Security Council. <https://undocs.org/S/2019/171>.

²⁸ N/A. (n.d.). Talent Ace. International Labour Organization Database on Reported Incidents of Abandonment of Seafarers.

https://www.ilo.org/dyn/seafarers/seafarersbrowse.details?p_lang=en&p_abandonment_id=351&p_search_id=201019195352.

²⁹ N/A. (2021, April 13). Talent Ace - IMO 9485617. ShipSpotting.com.

<http://www.shipspotting.com/gallery/photo.php?lid=3280537>.

³⁰ South Korean port records seen by the authors.

³¹ N/A. (2018, March 5). S/2018/171. United Nations Security Council. <https://www.undocs.org/S/2018/171>.

³² N/A. (2018, March 5). S/2018/171. United Nations Security Council. <https://www.undocs.org/S/2018/171>.

³³ <https://www.nknews.org/2021/08/south-korea-detaining-north-korea-linked-ship-suspected-of-sanctions-violations/>.

³⁴ The KINGSWAY was sanctioned for transferring fuel to the RYE SONG GANG 1 (IMO 7389704), a North Korean tanker, in violation of UNSC Resolutions 2375 and 2397. Source: N/A. (2017, December 28). Security Council Committee Established Pursuant to Resolution 1718 (2006) Designates 4 Vessels Pursuant to Paragraph 6 of Resolution 2375 (2017). United Nations Security Council. <https://www.un.org/press/en/2017/sc13149.doc.htm>.

³⁵ N/A. (2020, June 4). 1718 Designated Vessels List. United Nations Security Council.

https://www.un.org/securitycouncil/sites/www.un.org.securitycouncil/files/1718_designated_vessels_list_final.pdf.

³⁶ Strong, M. (2018, January 20). Taiwan Coast Guard Boards Ship in North Korea Investigation. Taiwan News.

<https://www.taiwannews.com.tw/en/news/3345749>.

³⁷ According to IHS Markit, the China-registered Taizhou Zhesheng Shipping Co., Ltd. was the first recorded owner and manager of the UNI WEALTH and Taizhou Haizhou Shipping Co., Ltd. of the ALPHA. Source: N/A. (n.d.). IHS Markit Maritime Intelligence Risk Suite (MIRS). IHS Markit. <https://mirs.maritime.ihs.com>.

³⁸ The graphic compares the *registered lengths* of the four vessel identities, which is a different type of measurement from the *length overall* (LOA). According to IHS Markit, neither the UNI WEALTH/APEX or ALPHA/W STAR identities listed a length overall. For more information about the difference between a vessel's registered length and length overall, see:

<https://www.dco.uscg.mil/Portals/9/DCO%20Documents/Marine%20Safety%20Center/Tonnage/2016%20Current%20Tonnage%20Regulations.pdf?ver=2017-06-09-123755-290>.

³⁹ N/A. (n.d.). W STAR. Equasis. <https://equasis.org>.

⁴⁰ N/A. (n.d.). IHS Markit Maritime Intelligence Risk Suite (MIRS). IHS Markit. <https://mirs.maritime.ihs.com>.

⁴¹ N/A. (n.d.). W STAR. Equasis. <https://equasis.org>.

⁴² The graphic measures the vessels' length overall (LOA). According to IHS Markit, the LOA of the KINGSWAY is 115.44 meters. Source: N/A. (n.d.). IHS Markit Maritime Intelligence Risk Suite (MIRS). IHS Markit. <https://mirs.maritime.ihs.com>.

⁴³ N/A. (2021, January 13). SHUN FA. VesselFinder. <https://www.vesselfinder.com/ship-photos/670222>.

⁴⁴ O'Carroll, C., Kim, J., & Jung, W.-G. (2021, August 20). *South Korea Detaining North Korea-linked Ship Suspected of Sanctions Violations*. NK News. <https://www.nknews.org/2021/08/south-korea-detaining-north-korea-linked-ship-suspected-of-sanctions-violations/>.

⁴⁵ N/A. (2020, March 2). S/2020/151. United Nations Security Council. <https://undocs.org/S/2020/151>.

; N/A. (2021, March 4). S/2021/211. United Nations Security Council. <https://undocs.org/S/2021/211>.

⁴⁶ The following case study used AIS data from Windward.

⁴⁷ N/A. (2018, February 27). Suspicion of Illegal Ship-to-Ship Transfers of Goods by CHON MA SAN, North Korean-flagged Tanker, and XIN YUAN 18, Maldivian-flagged Tanker. Ministry of Foreign Affairs of Japan. https://www.mofa.go.jp/fp/nsp/page4e_000775.html.

⁴⁸ N/A. (2018, February 27). Suspicion of Illegal Ship-to-Ship Transfers of Goods by CHON MA SAN, North Korean-flagged Tanker, and XIN YUAN 18, Maldivian-flagged Tanker. Ministry of Foreign Affairs of Japan. https://www.mofa.go.jp/fp/nsp/page4e_000775.html.

⁴⁹ Baidu Maps.

⁵⁰ According to IHS Markit, the SMOOTH SEA 22 was launched from Fujian Yihe's shipyard on 25 September 2018 and entered into service on 3 October 2018. The SMOOTH SEA 22's launch date was likely set to align with the SMOOTH SEA 28's arrival at the shipyard. Notably, the SMOOTH SEA 22 was also reportedly assigned a hull number "YH1717" by Fujian Yihe. Source: N/A. (n.d.). *IHS Markit Maritime Intelligence Risk Suite (MIRS)*. IHS Markit. <https://mirs.maritime.ihs.com>.

⁵¹ IHS Markit Maritime Intelligence Risk Suite (MIRS), n.d., <https://mirs.maritime.ihs.com>.

⁵² IHS Markit Maritime Intelligence Risk Suite (MIRS), n.d., <https://mirs.maritime.ihs.com>.

⁵³ IHS Markit Maritime Intelligence Risk Suite (MIRS), n.d., <https://mirs.maritime.ihs.com>.

⁵⁴ N/A. (n.d.). Milyan R Trade International Co. Ltd. (邁源紅貿易國際有限公司). Integrated Companies Registry Information System (ICRIS). <https://icris.cr.gov.hk>.

⁵⁵ A joint investigation by C4ADS and the Royal United Services Institute (RUSI) found that DPRK-linked tankers often traveled to waters in and around the Taiwan Strait to load oil bound for North Korea via STS transfers. For more information, see Kuo, L., Sung, L., Byrne, J., & Byrne, J. (2021, March 22). *Black Gold: Exposing North Korea's Oil Procurement Networks*. C4ADS. <https://c4ads.org/black-gold>.

⁵⁶ N/A. (2019, March 12). S/2019/171. United Nations Security Council. <https://www.undocs.org/S/2019/171>.

⁵⁷ N/A. (2002, December 12). *Amendments to the Annex to the International Convention for the Safety of Life at Sea (SOLAS), 1974*. Admiralty and Maritime Law Guide. <http://www.admiraltylawguide.com/conven/amendsolas2002.pdf>.

⁵⁸ There are two main types, or classes, of AIS transponders: Class A and Class B. Both classes transmit a vessel's static and dynamic information, but Class A transponders have additional functions required by the IMO that enable the vessel to conform to international maritime protocols and operate safely on the high seas. Class B transponders are not fully compliant with IMO requirements but confer the navigational benefits of AIS to users at a lower cost. Due to their technical configurations, Class B transponders typically have lower range and transmit with less frequency than Class A transponders. Notably, Class A AIS messages can include the vessel's IMO number; Class B AIS messages do not.