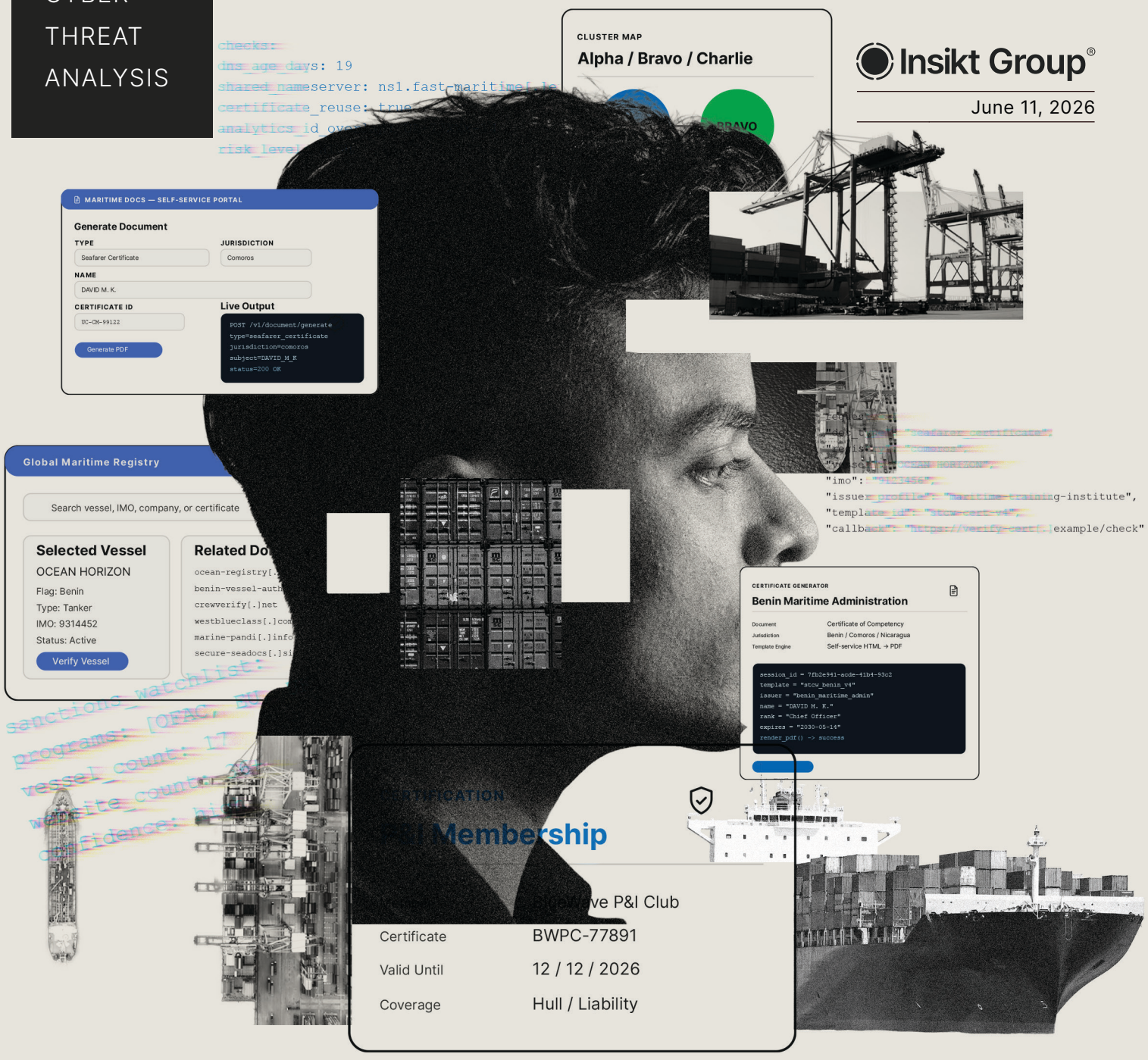
CYBER THREAT ANALYSIS

Recorded Future®

Insikt Group®

June 11, 2026



Cyber-Enabled Maritime Sanctions Evasion

Iranian and Russian shadow fleet vessels are likely using over 36 inauthentic websites in three distinct clusters designed to facilitate sanctions evasion.

Insikt Group identified inauthentic websites impersonating ship registries, national maritime administrations, STCW organizations, and ship classification societies, effectively replicating key layers of the maritime compliance stack.

Organizations in the maritime and shipping sectors should integrate independent verification and cyber threat intelligence into compliance workflows to proactively identify fraudulent online infrastructure.

Executive Summary

Iranian and Russian shadow fleet[1] vessels, along with multiple sanctions evasion networks (SENs), are using online infrastructure likely designed to facilitate sanctions evasion. The infrastructure consists of inauthentic websites impersonating ship registries, national maritime administrations, seafarer training and certification organizations, protection and indemnity (P&I) clubs, and ship classification societies, effectively replicating key layers of the maritime compliance stack. The websites are likely being used to circumvent maritime compliance mechanisms by generating and corroborating false documents and certificates.

The online infrastructure is consistent with a service-provider model in which threat actors offer reusable digital infrastructure, documentation, and identities, rather than operating as centrally coordinated, country-specific networks. Three identified clusters of online activity — designated as Alpha, Bravo, and Charlie for the purposes of this report — have several technical overlaps, suggesting these clusters may form a broader, loosely connected ecosystem of online infrastructure supporting multiple SENs. This activity also aligns with prior reporting by Bellingcat and Lloyd's List and demonstrates potential links between the two reports across these three clusters.

This infrastructure blends established sanctions evasion practices, such as exploiting weak jurisdictional oversight in under-resourced jurisdictions to conduct fraudulent ship flag registrations, with increasingly cyber-enabled tactics such as automated document generation and layered infrastructure to produce fraudulent documents and credible front companies, complicating detection and enforcement.

Cyber-enabled SENs almost certainly undermine sanctions compliance mechanisms by developing credible but fraudulent maritime organizations, increasing the risk of due diligence failures and regulatory exposure. Organizations in the maritime and shipping sectors should integrate independent verification and cyber threat intelligence into compliance workflows to proactively identify fraudulent online infrastructure. Governments whose authorities are regularly impersonated by SENs and associated service providers should prioritize coordinated identification and disruption of fraudulent infrastructure, particularly where threat actors claim multi-jurisdictional legitimacy.

[1] The International Maritime Organization (IMO) stated that *dark fleet* or *shadow fleet* means "ships that are engaged in illegal operations for the purposes of circumventing sanctions, evading compliance with safety or environmental regulations, avoiding insurance costs, or engaging in other illegal activities" (https://www.europarl.europa.eu/RegData/etudes/BRIE/2024/766242/EPRS_BRI(2024)766242_EN.pdf).

Key Findings

- SENs tied to the Iranian and Russian shadow fleets are likely using over 36 inauthentic websites in three distinct clusters. Insikt Group identified explicit connections between these websites and seventeen vessels, the majority of which have already been sanctioned by the United States (US) Department of the Treasury (USDT)'s Office of Foreign Asset Control (OFAC) and by other countries.
- Inauthentic websites identified as part of these clusters routinely impersonate national maritime administrations and ship registries from countries such as the Comoros and Benin, as well as Bhutan, Cameroon, Chad, Equatorial Guinea, Gambia, Haiti, Malawi, Nicaragua, and Zambia.
- Other websites also aim to establish fictional ship classification societies as credible registered organizations (ROs), in addition to several websites acting as fictional seafarer training and certification organizations and P&I clubs.
- One website impersonates the Benin Maritime Administration and provides a self-service tool to generate fraudulent seafarer documents from the governments of Benin, the Comoros, and Nicaragua.
- Attribution for at least two of the clusters documented in this report includes Cluster Alpha, which is likely to have been at least partially developed by an Indian web development company, Oceaniek Technologies. Cluster Bravo is linked to two Syrian nationals, one of whom has previous historical involvement in illicit activity. Cluster Charlie remains unattributed, although it shares technical and design characteristics with Cluster Bravo.

Table of Contents

Background

Three partially overlapping clusters of online infrastructure are likely being used by both the Iranian and Russian shadow fleets to evade sanctions (**Figure 1**). The three clusters (designated Alpha, Bravo, and Charlie) are connected through shared infrastructure, consistent domain registration patterns, and recurring operational security (OPSEC) mistakes.

The activity described in this report also overlaps with two previously unconnected activity clusters described by Bellingcat and Lloyd's List — the first tied to Indian web development company Oceaniek Technologies, and the second to a cluster of fraudulent ship registries centered around the domain *marinegov[.]net*. This activity also aligns with prior reporting from independent researcher Christian Panton, who collaborated with both Bellingcat and Lloyd's List.

Unlike traditional intrusion sets, these websites enabling maritime fraud and sanctions evasion form a complex network involving front companies, individuals, and vessels. However, Insikt Group has established initial attribution to one of the clusters to two Syrian nationals, with one individual having a record of previous involvement in illicit activities.

***Figure 1**: Clusters identified by Insikt Group (Source: Recorded Future)*

Summary of Tactics, Techniques, and Procedures (TTPs)

The online activity investigated in this report uses TTPs that likely reflect efforts by highly adaptive service providers and SENs to improve their flexibility and resilience following international sanctions and other enforcement actions. Overlapping and notable TTPs observed across these clusters include the following:

- **Exploiting weak jurisdictional oversight:** Networks consistently target countries with weaker maritime oversight to conduct flag fraud. Inauthentic websites flagged by Insikt Group in this report have repeatedly impersonated the governments of the Comoros and Benin, as well as those of Bhutan, Cameroon, Chad, Equatorial Guinea, Gambia, Haiti, Malawi, Nicaragua, and Zambia. Fraudulent ROs often claimed to be associated with multiple jurisdictions at once to build credibility and complicate enforcement.

- **Typosquatting and identity spoofing**: Inauthentic websites from all three clusters typosquat or impersonate legitimate national maritime administrations and ship registries to appear credible. Impersonation attempts also included reusing document templates from legitimate ship registries and impersonating specific staff email addresses (Cluster Alpha), or stealing visuals from maritime technology companies (Cluster Bravo).

- **Automated document forgery**: Cluster Alpha contained a self-service seafarer certificate generation tool to produce PDF documents and QR codes, impersonating documents from three jurisdictions. QR codes very likely facilitate the presentation and verification of documents during inspections to circumvent enforcement.

- **Building social media brands**: Cluster Bravo websites posing as ship classification societies set up social media accounts on mainstream platforms with consistent brand identities, likely to establish themselves as credible and legitimate organizations.

- **Mutual endorsements**: Cluster Charlie uses websites posing as national maritime administrations and ship registries to certify other websites within the same cluster, which in turn pose as classification societies and official ROs. The supposed ROs also link to each other as "partners" and link back to the purported ship registries for validation. This creates a mutual endorsement and validation loop designed to build credibility and manipulate search engines.

Initial Investigation

Based on reporting by Lloyd's List on the Iranian shadow fleet, Insikt Group identified several inauthentic websites claiming to be administrators of Beninese flags and impersonating the Benin Maritime Administration (*beninmaritime[.]org, beninmaritime[.]co, beninmaritime[.]net*), not included in Lloyd's original investigation. Research on the Benin Maritime Administration websites revealed no links to official Benin government domains or to Benin's National Portal of Public Services. Additionally, the IMO's Global Integrated Shipping Information System (GISIS) lists Benin's national point of contact for ship registries as the Direction des Affaires Portuaires, Maritimes et Fluvio-Lagunaires ("Directorate of Port, Maritime and River-Lagoon Affairs"), which is part of the Ministère du Cadre de Vie et des Transports (*cadredevie[.]gouv[.]bj*). The three inauthentic Benin Maritime Administration websites suggest that its authority falls under the Ministère Des Travaux Publics et Des Transports, which does not exist, according to the Benin government's ministries website.

The Benin Maritime Administration is not identified in GISIS as an RO representing Benin (there are no ROs listed for Benin). GISIS lists a physical address, two phone numbers, and three emails as Benin's national point of contact for ship registries; the fraudulent Benin Maritime Administration lists only a BP number ("Boîte Postale" or Post Office Box). One of the fraudulent websites also provides a typosquatted version of a real email address listed for Benin on GISIS (*gmahissou[@]gouv[.]bj* is spoofed as *gmahissou[@]guve[.]bj*).

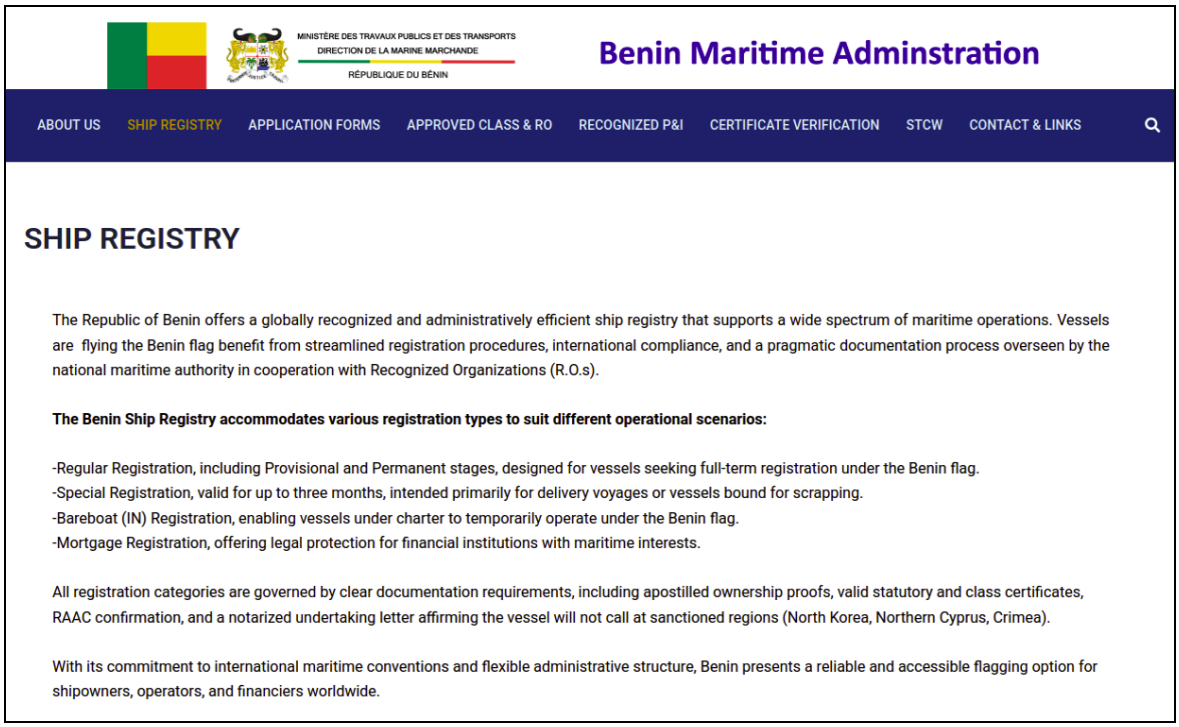


Figure 2: *Screenshot from the Benin Maritime Administration website offering Benin flag registration (Source: beninmaritime[.]org/ship-registry)*

Cluster Alpha

Cluster Alpha includes eleven websites linked to Insikt Group's initial investigation into inauthentic websites impersonating Benin government organizations. These websites impersonate ship registries and maritime administrations from Nicaragua and Benin, with the majority of the domains registered between June and October 2025:

- *atlasregister[.]net*
- *atlasregister[.]org*
- *beninmaritime[.]bj*
- *beninmaritime[.]net*
- *epnicaragua[.]com*
- *epnicaragua[.]org*
- *gove[.]bj*
- *guve[.]bj*
- *niataregister[.]net*
- *niataregister[.]org*

Links to Oceaniek Technologies

Insikt Group identified PDF documents uploaded to one website in this cluster, *epnicaragua[.]org*, that contain metadata, including the document's creation timestamps (with a +5:30 timezone specifier, likely referring to Indian Standard Time), as well as document authors and creators. Oceaniek Technologies (*oceaniektechnologies[.]com*) is an Indian web development company listed throughout the documents as the document authors or creators. Through similar methods, Bellingcat investigators previously identified *niataregister[.]org* and Oceaniek Technologies as part of an investigation into inauthentic websites linked to an individual accused of issuing false flag certificates to support illicit activity. This individual is also listed as the managing director of Oceaniek. This corroborates Insikt Group's findings for documents found on *epnicaragua[.]org*, and likely indicates that both websites were designed by Oceaniek; however, the websites' actual operators remain unclear.

Fraudulent Certificate Generation Tool

Insikt Group found multiple similar files shared by three of the Oceaniek-attributed websites (*bma[.]gov[.]bj*, *beninmaritime[.]net,* and *beninmaritime[.]bj*) and four other websites with similar names masquerading as the Benin Maritime Administration (and one website impersonating Zambia's ship registry) but with different hosting arrangements. Both *beninmaritime[.]net* and *beninmaritime[.]co* list their contact email addresses as *info[@]beninmaritime[.]org*, reinforcing the hypothesis that these websites are operated by the same threat actors:

- *beninmaritime[.]co*
- *beninmaritime[.]in*
- *beninmaritime[.]org*
- *registry[.]zmgov[.]org*

In October 2025, *pdf[.]beninmaritime[.]co* displayed a "Certificate PDF Generator" (**Figure 3**).

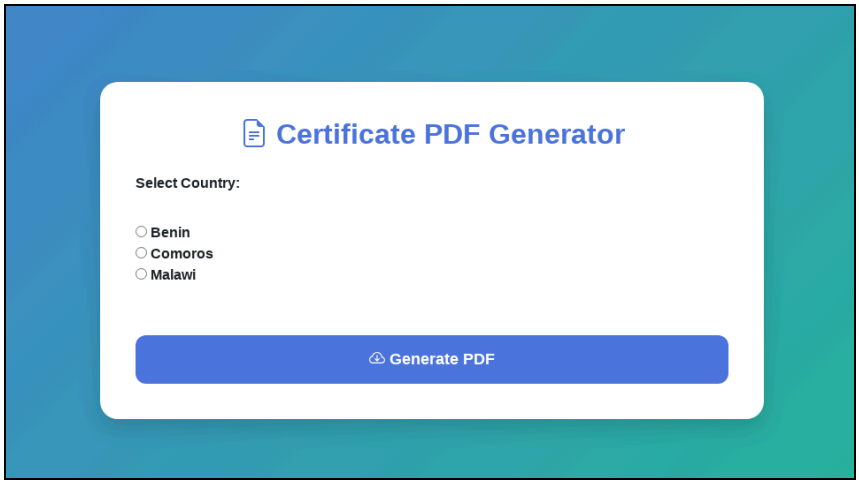


***FIgure 3**: Certificate PDF generator displayed on pdf[.]beninmaritime[.]co in October 2025 (Source: Recorded Future)*

As seen in the "Certificate PDF Generator" hosted on the subdomain in October 2025, a Django app in the open directory contains code to inject data from user-submitted forms into template documents for Benin, Comoros, and Malawi and export the results as PDF files (**Figure 4**). The app also generates QR codes linking to the PDF files on the *beninmaritime[.]co* website, likely for seafarers to easily display their fraudulent certification documents during inspections.

```
if country=="benin":
    raw_replacements = {
        "[[name]]": data.get("name"),
        "[[ship_name]]": data.get("ship_name"),
        "[[nationality]]": data.get("nationality"),
        "[[passport_no]]": data.get("passport_no"),
        "[[dob]]": data.get("dob"),
        # "[[certificate_no]]": data.get("certificate_no"),
        # "[[certificate_no2]]": data.get("certificate_no2"),
        # "[[government_of]]": data.get("government_of"),
        # "[[until]]": data.get("until"),
        # "[[until12]]": data.get("until"),
        "[[capacity]]": data.get("capacity"),
        "[[issuance_date]]": data.get("issuance_date"),
        "[[expiration_date]]": data.get("until"),
        "[[expiration date]]": data.get("until"),
    }
```

***Figure 4**: Code snippet from the Django web application injecting user-submitted data into templates (Source: Recorded Future)*

The web application directory contains PDF templates for seafarer certification documents for maritime administrations in Malawi, Comoros, and Benin:

UNION DES COMORES
Unité - Solidarité - Développement
ADMINISTRATION MARITIME

UNION OF COMOROS
Unity - Solidarity - Development
MARITIME ADMINISTRATION

PERMISSION ISSUED UNDER THE PROVISIONS OF REGULATION I/10 OF THE INTERNATIONAL CONVENTION ON STANDARDS OF TRAINING CERTIFICATION AND WATCHKEEPING FOR SEAFARERS 1978, AS AMENDED IN 1995.

Certificate N: MIP 24267144

The Maritime Administration of the Union of Comoros, permits

To: Fabio Vitionym
To serve with the capacity of: 141077
With Limitations: Ambivalent.
COC Number: IMO 271828182
Issuing Authority: ComoMar
On board of M/V: Water Sparrow
IMO Number: 42O6I337

for a period of three months, as a holder of a valid Appropriate Certificate, and as an officer who has deposited to our Administration his application for the issuance of relative recognition certificate under the provisions of the STCW'95.

Date of Issue : 10/04/2025

Naïri Abasse
Maritime commissioner

Form No. CRA/00_01

Date of issuance: 01/2019

***Figure 5**: Example fraudulent seafarer certificate spoofing the Comoros (Source: Recorded Future)*

Ties to Sanctioned Vessels

The open directory on *pdf[.]beninmaritime[.]co* contains over 30 fraudulent documents generated by the tool and certifying Pakistani, Indian, Russian, and Bangladeshi crew tied to sanctioned vessels that are likely part of the Russian shadow fleet, with the following ship names, IMO numbers, and flags recorded in the certificates:

Ship Name	IMO	Flag	Sanctions
SOFIA K	9299123	Panama	Sanctioned as part of the Russian shadow fleet by the United Kingdom (UK), Ukraine (UA), Canada (CA), European Union (EU), and Switzerland (CH)
MAISAN	9289776	Benin	Sanctioned by OFAC as part of the Russian shadow fleet and facilitating oil transfers to Houthis
DIANCHI	9281011	Comoros	Sanctioned as part of the Russian shadow fleet by OFAC, UK, UA, CA, Australia (AUS), EU, and CH
BAISHA	9436941	Russia	Sanctioned as part of the Russian shadow fleet by OFAC, UK, UA, CA, AUS, EU, CH
STABILIS I	9234501	Benin	Sanctioned as part of the Russian shadow fleet by UK, UA, CA, EU, CH, AUS

Ship Name	IMO	Flag	Sanctions
OLAF I	9224465	Comoros	Sanctioned as part of the Russian shadow fleet by OFAC, UK, UA, EU, CH
BOLTARIS	9251456	Benin	Sanctioned as part of the Russian shadow fleet by UA, UK, CA, AUS, CH, EU

Table 1: *Sanctioned vessels found in fraudulent seafarer documents on pdf[.]beninmaritime[.]co; names are displayed as recorded in identified documents*

Several of these vessels (MAISAN, DIANCHI, BAISHA, and SOFIA K) were once managed by Gatik Ship Management, an Indian company accused of becoming "the largest carrier of Russian oil" since the start of the Russia-Ukraine war. Insikt Group has also identified likely common ownership between BOLTARIS, STABILIS I, and OLAF I, with the former having been linked via intermediaries to PJSC Sovcomflot, the "largest state-owned shipping company in Russia." The three vessels also exhibit common registration patterns via front companies registered in the Seychelles, India, and the United Arab Emirates (UAE):

Name	Registered Owner	ISM Manager
BOLTARIS	Trident Serenity Ltd. (Seychelles)	Maritime Maven Management Ltd. (UAE)
STABILIS I	Trident Trinity Ltd. (UAE)	Maritime Maven Management Ltd. (UAE)
OLAF I	Trident Infinity Ltd. (India)	Vigor Marine Services LLP (India)

Table 2: *Vessels included in the documents using front companies with consistent naming conventions*

Via these "Trident"-themed shell companies and shared International Safety Management (ISM) managers, Insikt Group was able to identify further oil tankers likely also involved in Russian shadow fleet activity:

Name	Registered Owner	ISM Manager
LIGERA	Trident Liberty Ltd. (Malaysia)	Ultra Shipping SDN BHD
CELERIX	Trident Modesty Ltd. (Seychelles)	Maritime Maven Management Ltd. (UAE)
GRUS I	Trident Beauty Ltd. (India)	Vigor Marine Services LLP

Table 3: *Vessels using front companies with consistent naming conventions*

According to Automatic Identification System (AIS) data from the Recorded Future Intelligence Operations Platform, shadow fleet vessel activity since September 2025 spans a global network with itineraries between Russian Black Sea ports such as Novorossiysk and Tuapse and destinations such as

Venezuela and Port Said, Egypt. Other vessels link to Port Said from the coast of Oman and the UAE, just off the Strait of Hormuz, and one vessel, OLAF I, ferries between the Strait of Malacca and Port Said.

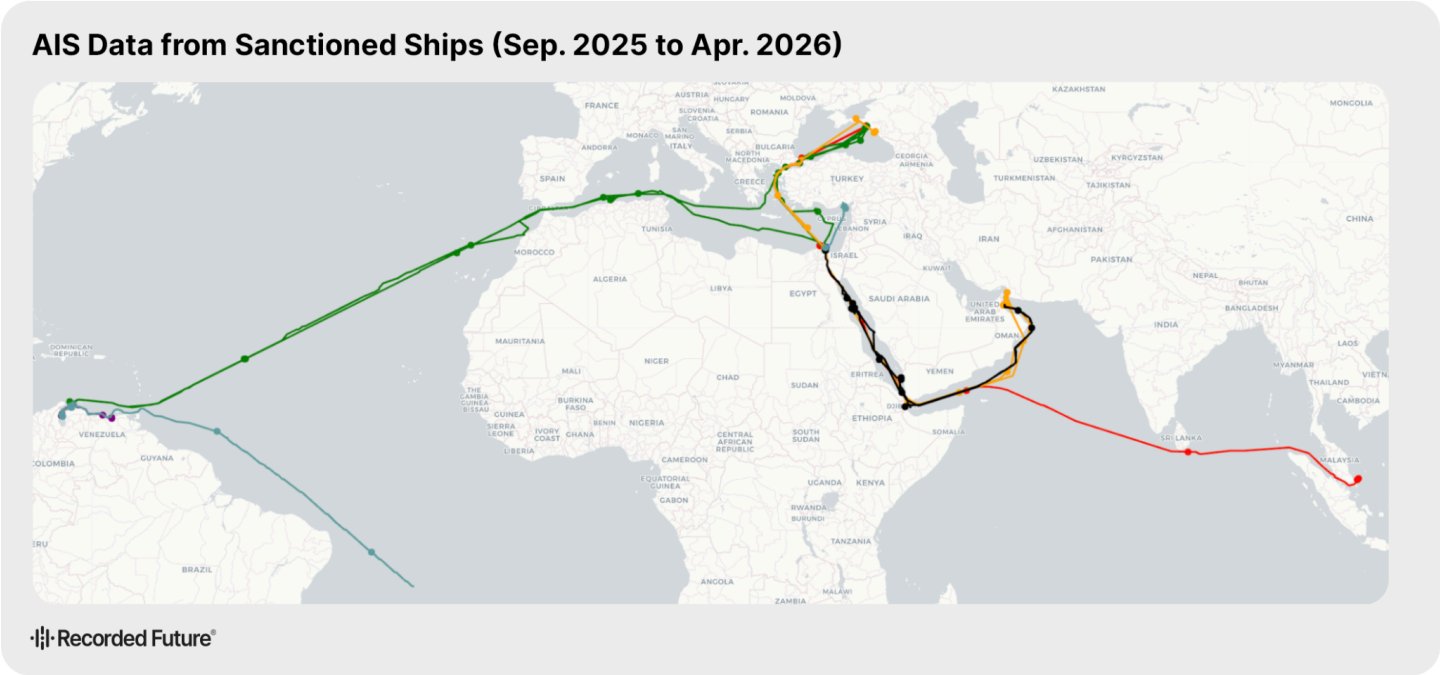


***Figure 6**: AIS data from sanctioned ships since September 2025, as of late April 2026 (Source: Recorded Future)*

Additionally, Insikt Group identified an image uploaded to the open directory named "tavian 1 windward.JPG" containing a screenshot (**Figure 7**) likely sourced from maritime intelligence platform Windward and likely depicting the itinerary of Russian "zombie tanker" TAVIAN I (IMO 1095337). The screenshot shows an itinerary between China (likely Shanghai), the Strait of Hormuz, and Germany (likely Kiel) between January and October 2025.

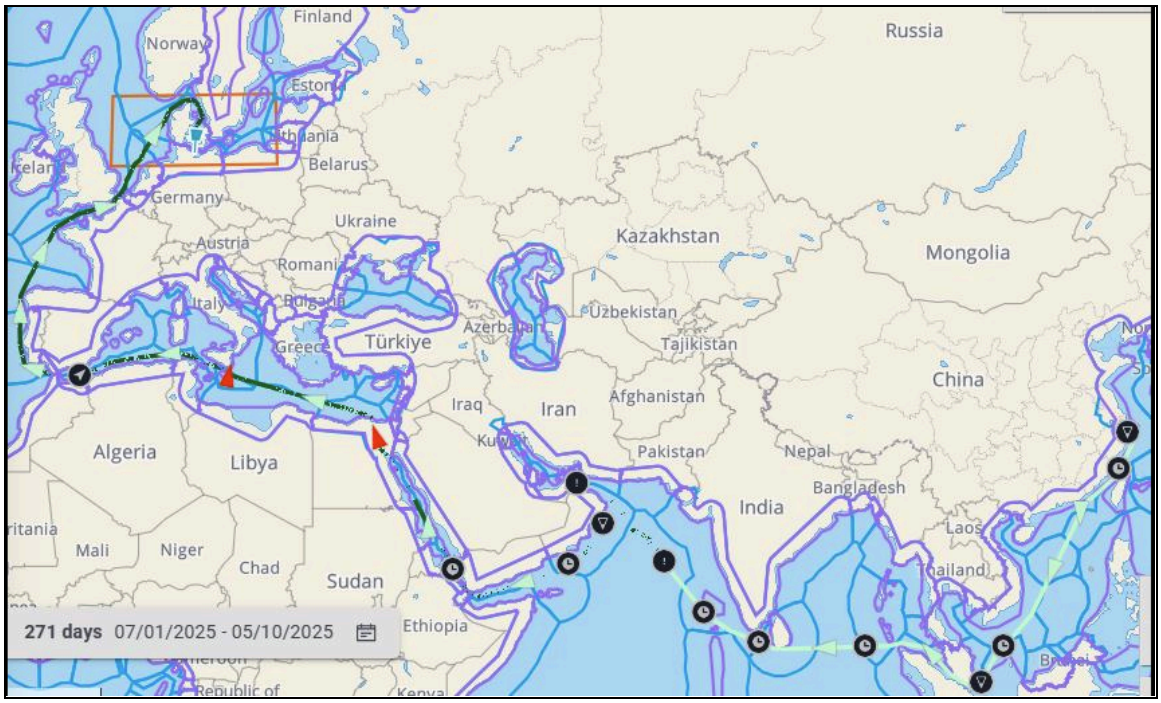


***Figure 7**: Windward Maritime AI Platform screenshot identified on pdf[.]beninmaritime[.]co (Source: Recorded Future)*

Metadata analysis of documents uploaded to the open directory lists two persons associated with Palau's Ship Registry. Insikt Group confirmed that these employees are also listed in the metadata for similar PDFs distributed on PISR's official website *palaureg[.]com*, which likely indicates that the operators behind *epnicaragua[.]org* reused the documents from PISR's official website as templates.

Seafarer certification templates found in the open directory impersonating maritime administrations in Benin, Comoros, and Malawi all include metadata listing the same individual as the document creator.

Cluster Bravo

Cluster Bravo includes seven websites using similar hosting and posing as maritime classification societies, seafarer training centers, and shipping registries. Insikt Group has identified online documents containing evidence that these websites have likely supported both Russian and Iranian shadow fleet sanctions evasion, suggesting that the operators of Cluster Bravo are likely an opportunistic service provider rather than directly embedded in either country's state-run sanctions evasion mechanisms. Websites identified in this cluster facilitate sanctions evasion by masquerading as:

- National maritime administrations and shipping registries (to issue fraudulent ship certificates)
- Seafarer training and certification centers (to issue fraudulent seafarer certificates, such as for IMO-mandated Standards of Training, Certification, and Watchkeeping [STCW] training)
- Classification societies (to issue fraudulent ship inspection certificates)

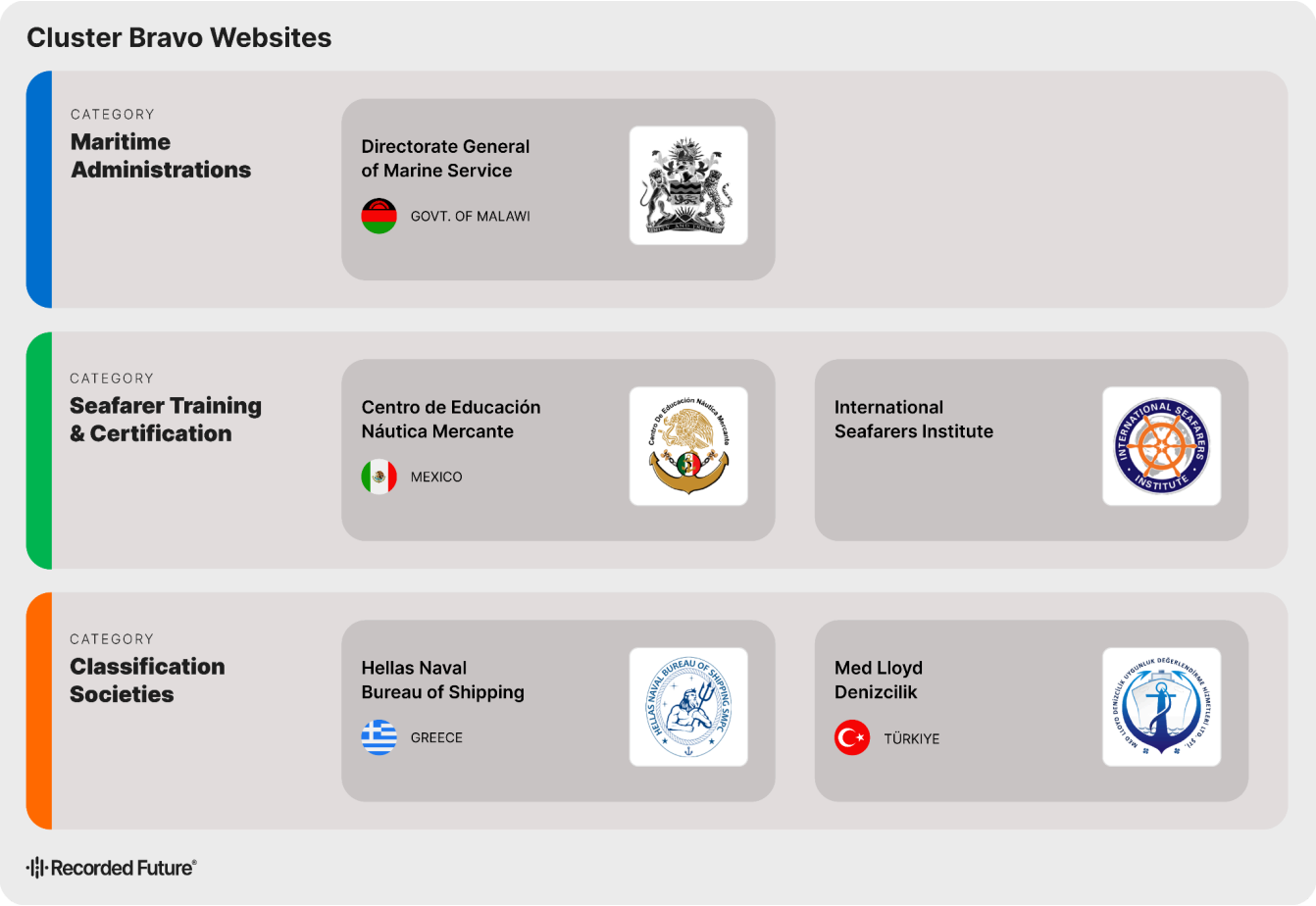


***Figure 8**: Cluster Bravo inauthentic website logos (Source: Recorded Future)*

Insikt Group identified evidence of ties between Cluster Bravo websites and two Syrian nationals based in Türkiye.

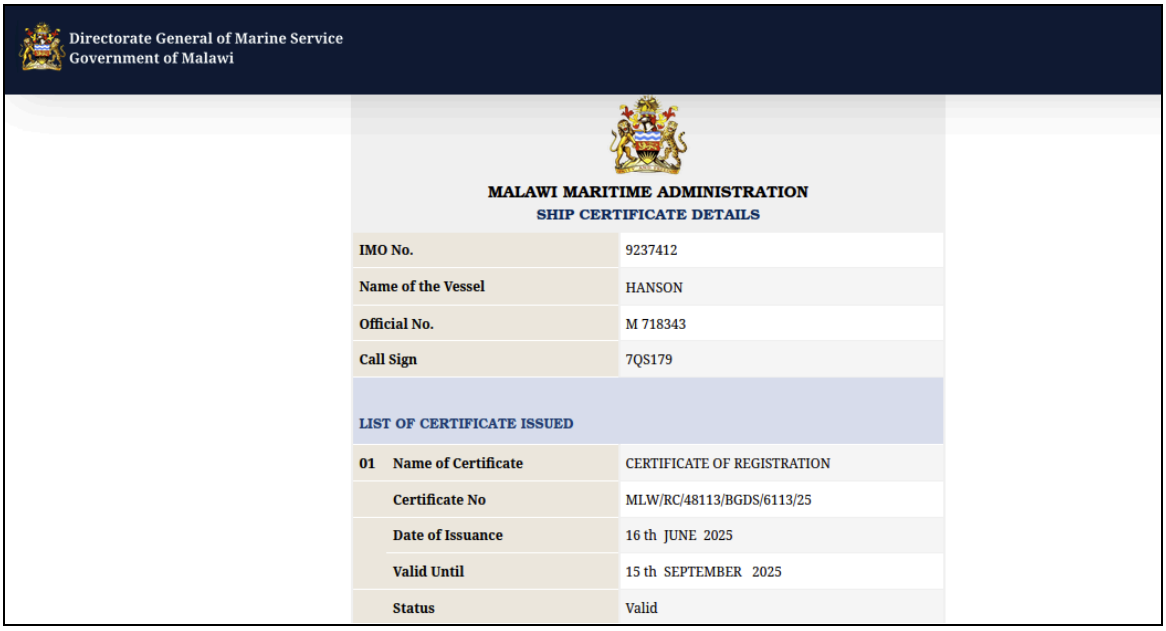
Links to Cluster Alpha

A subdomain on the Cluster Alpha website *beninmaritime[.]net*, *medlloyd[.]online[.]beninmaritime[.]net*, indicates a link to another domain hosted on different infrastructure, *medlloyd[.]online*. This domain is co-hosted on *159[.]198[.]36[.]123* with the following other maritime domains and is hosted on the same Namecheap IP range as Cluster Alpha domains, *159[.]198[.]0[.]0*/16:

- *isithin[.]com*
- *hellasnaval[.]net*
- *marinegov[.]org*
- *medlloyd[.]online*
- *medlloyd[.]org*
- *nauticacentro[.]com*
- *nauticacentro[.]mx*

Ship Registry

marinegov[.]org has several subdomains impersonating Malawi ship registry websites, *malawi[.]marinegov[.]org* and *malawi[.]shipregistry[.]marinegov[.]org*. By default, the latter displays a page showing ship certificates for the vessel HANSON (IMO 9237412), which was sanctioned by OFAC in March 2025 for transporting Iranian oil to China. In February 2026, the same ship was designated by the UK government for transporting Russian oil.



Directorate General of Marine Service
Government of Malawi

MALAWI MARITIME ADMINISTRATION
SHIP CERTIFICATE DETAILS

IMO No.	9237412
Name of the Vessel	HANSON
Official No.	M 718343
Call Sign	7QS179

LIST OF CERTIFICATE ISSUED

01	Name of Certificate	CERTIFICATE OF REGISTRATION
	Certificate No	MLW/RC/48113/BGDS/6113/25
	Date of Issuance	16 th JUNE 2025
	Valid Until	15 th SEPTEMBER 2025
	Status	Valid

***Figure 9**: Alleged ship certificate for sanctioned oil tanker HANSON displayed on an inauthentic website impersonating the government of Malawi (Source: malawi[.]shipregistry[.]marinegov[.]org)*

Ship Name	IMO Number	Flag	Sanctions
HANSON	9237412	Mozambique	Sanctioned as part of the Russian shadow fleet by US, UK, UA, CA, EU, CH, AUS

Table 4: *Information for sanctioned vessels linked to malawi[.]shipregistry[.]marinegov[.]org*

Maritime Training Centers

Centro de Educación Náutica Mercante

Two websites in Cluster Bravo, *nauticacentro[.]mx* and *nauticacentro[.]com*, are masquerading as a Mexican seafarer training and certification institute, the "Centro de Educación Náutica Mercante" ("CENM"). *nauticacentro[.]mx* is listed as an "approved maritime institute" on a website impersonating a Guyanese maritime administration, *imsag[.]org*.

The CENM websites claim that they provide IMO-mandated STCW training for seafarers, and host a queryable database of certificates issued to seafarers:

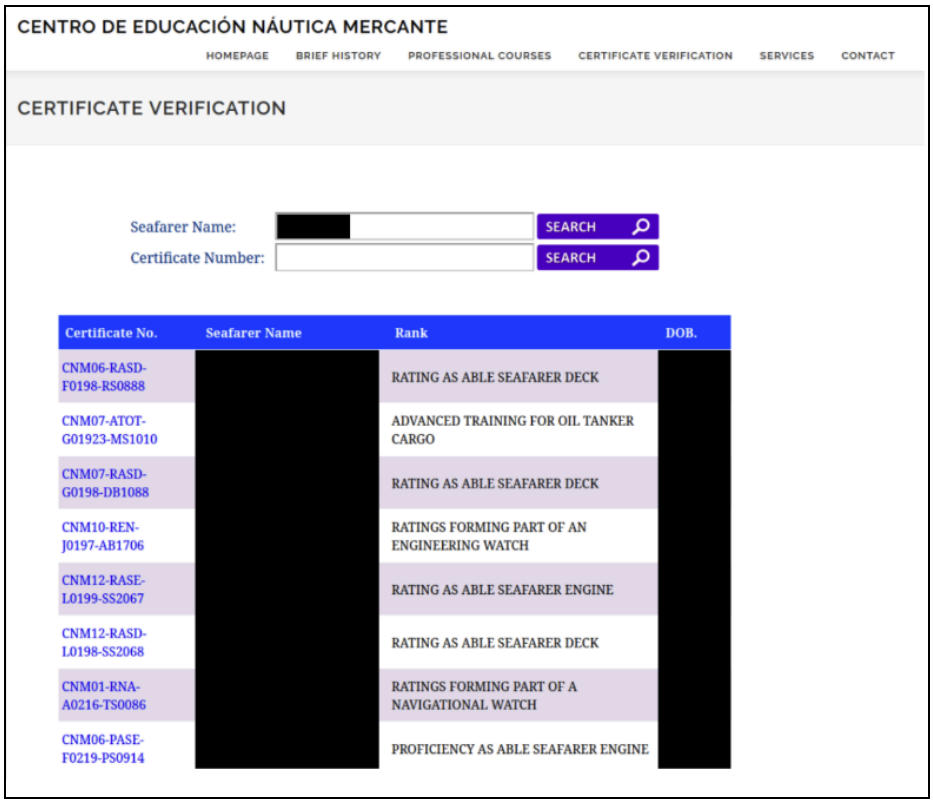


Figure 10*: CENM website containing an open database of seafarer certifications (Source: nauticacentro[.]mx)*

Insikt Group identified a document in an open source showing a course certificate issued by CENM in September 2023 for a Syrian national, claiming that the course was "approved" by the government of

Comoros. Insikt Group could not find any references to such an agreement or partnership between the country and CENM. The same source also included a PDF document for the same individual showing a confirmation of certification issuance by "International Marine Services" ("IMS") (*imsnaval[.]com*), another likely fraudulent organization that is part of Cluster Bravo. Both documents were likely scanned from physical documents using CamScanner, a mobile app that allows users to create PDFs from photographs.

Centro de Educación Náutica Mercante
Volcan Ajusco Street, Pradera C.P. 07500, Mexico City, Mexico
Tel: +52-5584215200 - Web: www.nauticacentro.mx - Email: info@nauticacentro.mx
Quality Management System Certified in accordance to ISO 9001:2015

Certificate Code: CNM09-REN-I0237-MH2087

Certificate of Completion
This Certificate is issued to

[redacted]

Nationality: SYRIA

For having satisfactorily completed the approved training courses in

Ratings Forming Part of an Engineering Watch
(40 Hours)

Accepted by General Directorate of Merchant Marine and has been deemed competent in accordance with the requirements of Regulations III/4, Section A-III/4 and Table A-III/4, of the International Convention on Standards of Training, Certification and Watchkeeping for Seafarers 1978 as amended in Manila 2010.

The course was conducted by Nautical Maritime Education Center, Mexico City, Mexico.

This course has been approved by the Government of Union of Comoros, Resolution No. 209/ANAM/DG

Date of Issuance: 21 SEPTEMBER 2023

Training Manager: Fernando J. Manuel García

Signature of Candidate: _____

ISO 9001 2015 CERTIFIED

The authenticity and validity of this certificate may be verified: certification@nauticacentro.mx

I.M.S
International Marine Services
TARTOUS - SYRIA - Tel: 00963-43-321850 / Fax: 00963-43-318343 / E-mail: stcw@imsnaval.com

Re: 1120/STCW/09/23 Date: 21.09.2023
TO: [redacted]

Confirmation of Issuance Certificates [redacted]

Dear Sirs,

This is to certify that the following certificates have been issued for;

1- [redacted]

- Ratings Forming Part of an Engineering Watch No. CNM09-REN-I0237-MH2087

Best Regards

Seafarers Department
International Marine Services

***Figure 11**: Certificates granted by CENM and IMS (Source: Recorded Future)*

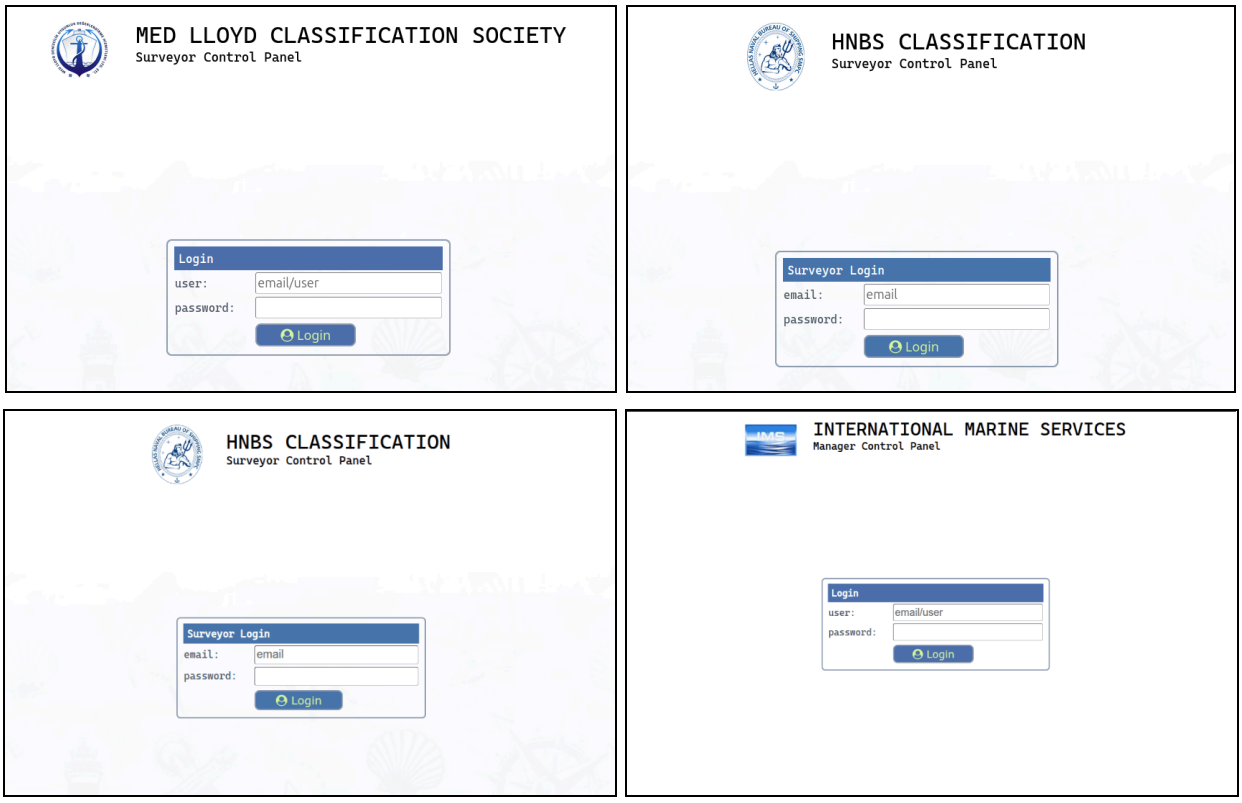
International Seafarers Institute

Insikt Group also identified *isithin[.]com* ("International Seafarers Institute", "ISI") as part of Cluster Bravo. Like CENM, ISI claims to provide STCW training but lists a Thai contact phone number and a stated address in Bangkok, Thailand.

***Figure 12**: ISI website banner (Source: isithin[.]com)*

Ship Classification Societies

Two of the domains in Cluster Bravo host login pages for likely fraudulent ship classification societies with ties to sanctioned vessels: Hellas Naval Bureau of Shipping (*hellasnaval[.]com,* "HNBS") and Med Lloyd Classification Society (*medlloyd[.]online*). Identical login pages are hosted on *hellasnaval[.]net[.]olymposnaval[.]com* and *imspanel[.]com,* with the latter having the HTTP title "Med Classification Society" but displaying "International Marine Services" ("IMS").



Figures 13, 14, 15, and 16*: Login panels for HNBS, Med Lloyd, and IMS (Source: urlscan.io — 1, 2, 3, 4)*

Classification societies help certify vessel safety and compliance with environmental regulations, and can act as ROs for IMO member states. Both Med Lloyd and HNBS are listed as ROs for Cameroon and Kenya. HNBS is also listed as an RO for the Comoros, Tanzania, and Kenya. Med Lloyd is listed as an RO for Benin on one of the fraudulent Benin websites in Cluster Alpha, *beninmaritime[.]net*, in addition to Gambia's legitimate maritime administration website.

Med Lloyd Classification Society

Med Lloyd Classification Society is likely an inauthentic ship classification society with two websites (*medlloyd[.]org* and *medlloyd[.]online*) registered in 2023. To aid in establishing its credibility, the company has a YouTube channel, Facebook page, Instagram account, and social media account, and claims to be located in Türkiye's largest container port, Mersin.

Hellas Naval Bureau of Shipping

Another website found in Cluster Bravo, *hellasnaval[.]net*, hosts a website similar to Med Lloyd and masquerades as a classification society named "Hellas Naval Bureau of Shipping" ("HNBS") based in Piraeus, Greece. IMSAG's fraudulent website also lists HNBS as an RO.

hellasnaval[.]net was first registered on December 4, 2019, shortly after the domain registration of another similarly themed domain, *hellasnaval[.]com*. The latter is hosted on the same IP range as *medlloyd[.]org* (66[.]96[.]128[.]0/18) and the two domains share the same PTR record, *150[.]160[.]96[.]66[.]static[.]eigbox[.]ne*.

Olymbos Naval

Insikt Group identified a third entity related to Med Lloyd and HNBS named "Olymbos Naval" (*olymposnaval[.]com*). While Olymbos's website is hosted on different infrastructure (*151[.]80[.]4[.]227*) than the other two entities' websites (*159[.]198[.]36[.]123*), the website's domain has the following subdomains pointing back to Med Lloyd, HNBS, and IMS:

- *hellasnaval[.]net[.]olymposnaval[.]com*
- *imspanel[.]com[.]olymposnaval[.]com*
- *medlloyd[.]online[.]olymposnaval[.]com*

Olymbos's website claims to provide data analysis and surveying services and features a screenshot of vessel design software likely stolen from a legitimate maritime software company, NAPA Studios.

Ties to Sanctioned Vessels

Insikt Group identified links between Med Lloyd Classification Society and HNBS and vessels tied to both the Iranian and Russian shadow fleets.

An April 2025 Sohu article by the Zhoushan Maritime Safety Administration (ZMSA) states that its December 23, 2024, inspection of SERANO II (IMO 9165542) found "that the vessel's inspection certificate had several non-compliant issues" and that "the QR code on the ship inspection certificate is displayed incorrectly." The article states that the ZMSA found that "the ship inspection agency 'MED LLOYD CLASSIFICATION SOCIETY' bears significant responsibility for the arbitrary issuance of statutory inspection certificates and the resulting detention." In November 2020, the non-governmental organization United Against Nuclear Iran (UANI) had flagged SERANO II as being likely part of the Iranian shadow fleet.

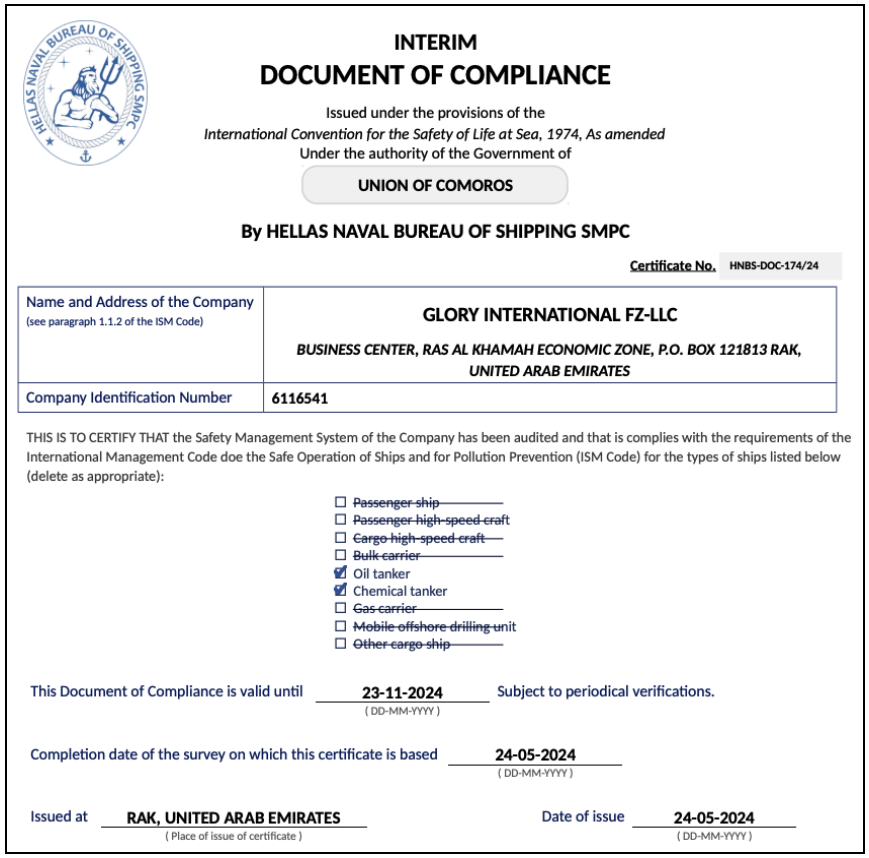
***Figure 17**: ZMSA officials examining SERANO II inspection certificates (Source: Sohu)*

Via Tokyo Memorandum of Understanding (MOU) vessel detention records identified in open sources, Insikt Group found that Med Lloyd Classification Society has been listed as the classification society for the following vessels with flags from Cameroon, the Comoros, and Gambia, including several vessels sanctioned or accused of being part of the Russian and Iranian shadow fleets:

Ship Name	IMO Number	Flag	Detentions / Sanctions
SERENA	9255660	Cameroon	Detained in March 2025 in Dalian, China, and in February 2026 in Dongjiakou, China Sanctioned as part of the Russian shadow fleet by UK, UA, CA, EU, CH, AUS
MAKMUR	9078189	Comoros	Detained in December 2025 in Singapore
TIS 520	9047300	Comoros	Detained in December 2025 in Singapore
PRS OCEAN	9276561	Gambia	Detained in August 2025 in Dongjiakou, China Sanctioned as part of the Russian shadow fleet by UK, UA, CA, EU, CH, AUS
KATSUYA	9178068	Gambia	Detained in February 2025 in Dongjiakou, China Sanctioned as part of the Iranian shadow fleet by OFAC
SERANO II	9165542	Gambia	Detained in December 2024 in Zhoushan, China Suspected to be part of the Iranian "Ghost Armada" by UANI

***Table 5:** Information for sanctioned vessels linked to Med Lloyd Classification Society*

Insikt Group identified a document via open sources (**Figure 18**) linking HNBS to sanctioned activity by certifying the UAE-based company Glory International FZ-LLC in May 2024. Glory International FZ-LLC was sanctioned by OFAC in April 2025, and is reportedly owned by an Indian national, who OFAC alleged "owns multiple shipping companies that boast a fleet of nearly 30 vessels [...] that have transported Iranian oil on behalf of the National Iranian Oil Company (NIOC) and the Iranian military." The document contains a QR code which links to *hellasnaval[.]net* with an empty Unique Tracking Number (UTN).



INTERIM
DOCUMENT OF COMPLIANCE

Issued under the provisions of the
International Convention for the Safety of Life at Sea, 1974, As amended
Under the authority of the Government of

UNION OF COMOROS

By HELLAS NAVAL BUREAU OF SHIPPING SMPC

Certificate No. HNBS-DOC-174/24

Name and Address of the Company (see paragraph 1.1.2 of the ISM Code)	GLORY INTERNATIONAL FZ-LLC *BUSINESS CENTER, RAS AL KHAMAH ECONOMIC ZONE, P.O. BOX 121813 RAK, UNITED ARAB EMIRATES*
Company Identification Number	6116541

THIS IS TO CERTIFY THAT the Safety Management System of the Company has been audited and that is complies with the requirements of the International Management Code doe the Safe Operation of Ships and for Pollution Prevention (ISM Code) for the types of ships listed below (delete as appropriate):

- ☐ ~~Passenger ship~~
- ☐ ~~Passenger high-speed craft~~
- ☐ ~~Cargo high-speed craft~~
- ☐ ~~Bulk carrier~~
- ☑ Oil tanker
- ☑ Chemical tanker
- ☐ ~~Gas carrier~~
- ☐ ~~Mobile offshore drilling unit~~
- ☐ ~~Other cargo ship~~

This Document of Compliance is valid until 23-11-2024 (DD-MM-YYYY) Subject to periodical verifications.

Completion date of the survey on which this certificate is based 24-05-2024 (DD-MM-YYYY)

Issued at RAK, UNITED ARAB EMIRATES (Place of issue of certificate) Date of issue 24-05-2024 (DD-MM-YYYY)

***Figure 18**: PDF document issued by HNBS to sanctioned entity Glory International FZ-LLC (Source: Archive)*

Via Tokyo and Abuja MOU vessel detention records identified in open sources, Insikt Group found that HNBS has been listed as the classification society for at least two bulk carriers and an oil tanker, all flying the Comoran flag:

Ship Name	IMO Number	Flag	Type / Detentions / Sanctions
GOLDEN LEO	9181833	Comoros	Bulk carrier detained in May 2021 in Port Kelang, Malaysia under Tokyo MOU
JAMILA	9083275	Comoros	Bulk carrier detained in September 2022 in Port Kelang, Malaysia under Tokyo MOU
BURAAQ	8914829	Comoros	Oil tanker detained under Abuja MOU

Table 6: *Information for sanctioned vessels linked to HNBS*

While Insikt Group was unable to ascertain the exact nature of HNBS-linked vessels' current operations, AIS location data indexed in the Recorded Future Intelligence Operations Platform shows that HNBS-linked bulk carrier GOLDEN LEO (9181833) made several trips between Syria, Türkiye, and Black Sea ports in Romania and Bulgaria since September 2025. AIS data for oil tanker BURAAQ indicates the tanker was between Gambia and Port Said, Egypt, from September 2025 to February 2026, with a trip toward the Gulf of Aden.

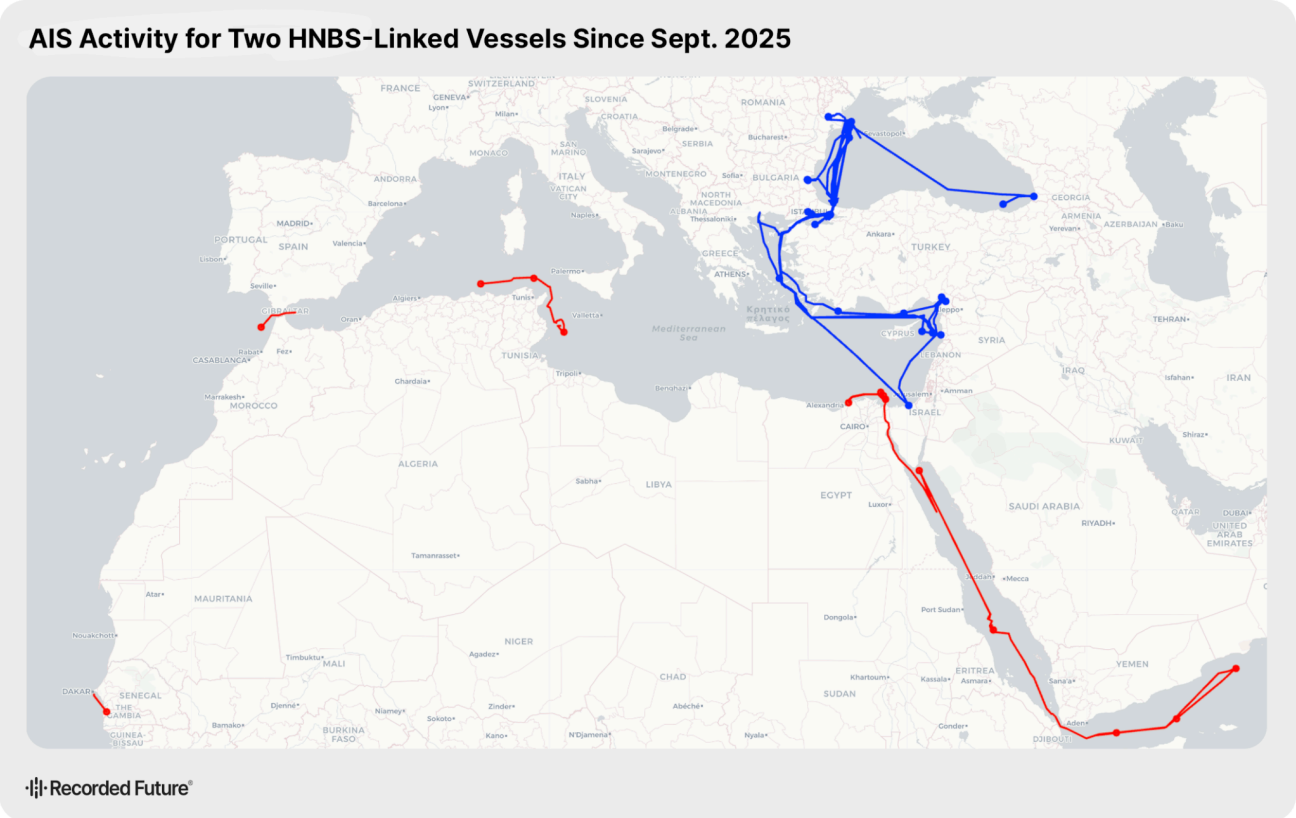


Figure 19*: AIS activity for HNBS-linked vessels GOLDEN LEO (blue) and BURAAQ (red) since September 2025 (Source: Recorded Future)*

Links to Marinegov Network

Insikt Group identified one domain in Cluster Bravo, *marinegov[.]org*, which shares naming conventions with a large network of websites and subdomains tied to *marinegov[.]net* (the "Marinegov" network) described by Lloyd's List in July 2025. One of the *marinegov[.]org* subdomains identified by Insikt Group, *malawi[.]shipregistry[.]marinegov[.]org*, hosts a website impersonating the Malawi Maritime Administration. The website lists *info[@]malawi[.]marinegov[.]net* as a contact email address, potentially indicating an OPSEC mistake by operators and linking back to Lloyd's List's investigation. However, we were unable to identify any additional links between clusters Alpha, Bravo, or Charlie and the Marinegov network to further substantiate this overlap.

Cluster Charlie

Unlike other clusters of inauthentic websites identified by Insikt Group, Cluster Charlie adopts a layered approach to establish credibility. At least fourteen inauthentic websites in this cluster impersonate ship registries from countries such as Bhutan, Brunei, Cameroon, Chad, Equatorial Guinea, Haiti, and Zambia. Several of these websites list two websites masquerading as legitimate vessel compliance and certification companies, *alliance-scs[.]org* ("Alliance Ship Classification Services", "ASCS") and *pioneersmaritime[.]com* ("Pioneers Maritime Ship Management", "PMSM" henceforth), as ROs. Both websites also claim to be ROs with flag authorizations from inauthentic websites in the same cluster, and PMSM lists ASCS as a "trusted partner" on its website. Several of the inauthentic websites also list PMSM or ASCS as ROs.

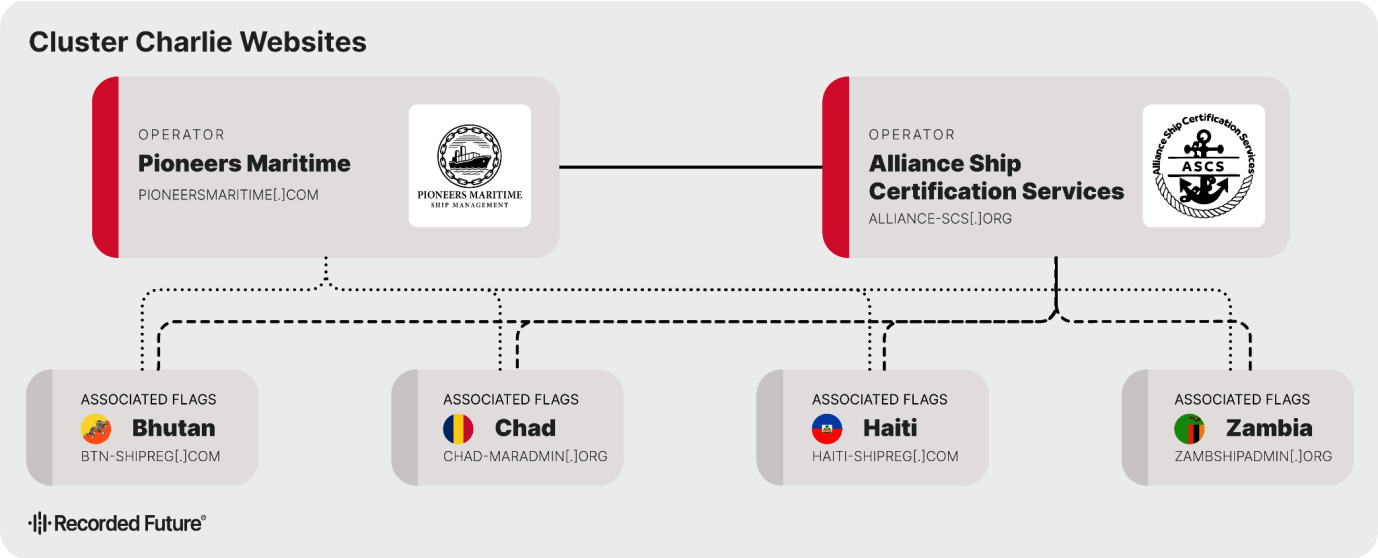
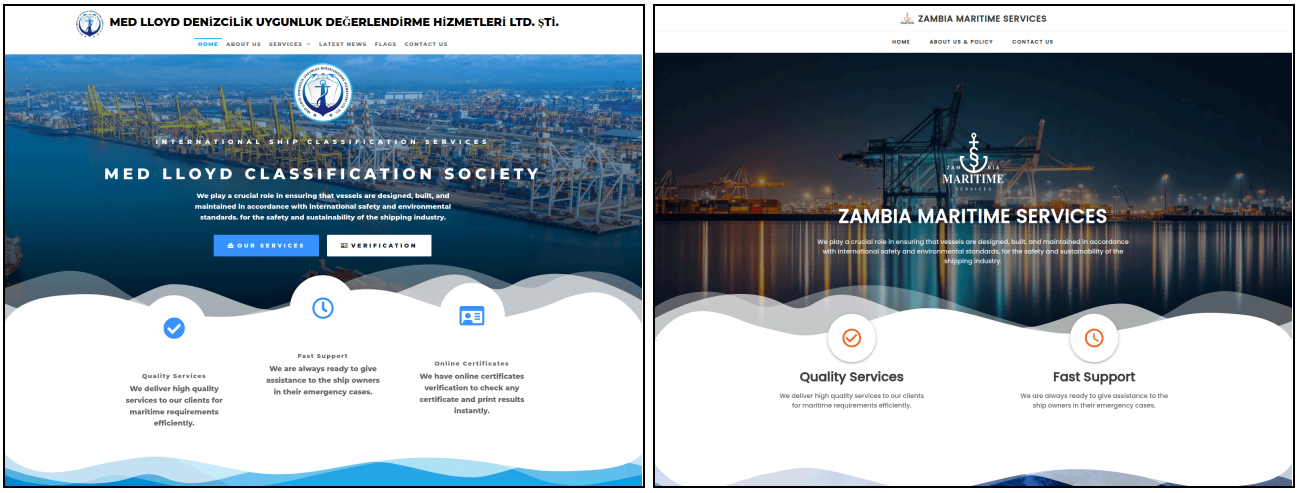


***Figure 20**: Cluster Charlie's layering technique, where inauthentic maritime administrations list other inauthentic websites masquerading as ship certification services (Source: Recorded Future)*

Links to Cluster Bravo

Insikt Group identified a likely fraudulent ship registry website impersonating the Zambian Maritime Administration (*zambiamaritime[.]org*) with a similar design to Med Lloyd's website (Cluster Bravo, *medlloyd[.]org*) and several identical files:



***Figures 21 and 22**: Screenshots of Med Lloyd's website, medlloyd[.]org (Left) and zambiamaritime[.]org (Right) (Source: urlscan.io — 1, 2)*

zambiamaritime[.]org is part of a larger cluster of at least fourteen inauthentic ship registry and classification society websites, all hosted on *217[.]76[.]51[.]133*. The websites also use similar login panels hosted on `admin.{domain}/login/`, and often link to each other.

- *alliance-scs[.]org*
- *benin-maritime[.]org*
- *brunieshipclass[.]org*
- *btn-shipreg[.]com*
- *cameroonshipregistry[.]org*
- *chad-maradmin[.]org*
- *eqguinea-shipadmin[.]org*
- *haiti-shipreg[.]com*
- *hss-registry[.]org*
- *mpabd-shipregistry[.]org*
- *pioneersmaritime[.]com*
- *sasmaa[.]club*
- *zambmaritime[.]org*
- *zambshipadmin[.]org*

Pioneers Maritime Ship Management

pioneersmaritime[.]com claims to be a maritime service provider named "Pioneers Maritime Ship Management" acting as an RO for Bhutan, Chad, the Comoros, Honduras, Haiti, Guinea-Bissau, and Saint Kitts and Nevis. The website's list of countries' alleged maritime administrations links to other websites in the network, including *haiti-shipreg[.]com*, *btn-shipreg[.]com*, and *chad-maradmin[.]org*. PMSM also lists a UAE mobile phone number, +97 1527294918, which is also listed on *haiti-shipreg[.]com*.

***Figure 23**: List of alleged recognized flag authorizations on pioneersmaritime[.]com (Source: Recorded Future)*

Another website in Cluster Charlie, *sasmaa[.]club* (masquerading as a P&I club named the South African Shipowners Mutual Assurance Association), lists "Pioneers Maritime Ship Management LLC", located in Dubai, UAE, as a "correspondent."

Alliance SCS

alliance-scs[.]org claims to be a classification society named "Alliance Ship Certification Services" ("Alliance SCS") based in Türkiye. Similar to Pioneers Maritime, Alliance SCS claims to be an RO for Bhutan, Chad, Haiti, and Zambia, and its website links to other inauthentic websites impersonating maritime administrations in this cluster.

***Figure 24**: Alliance SCS banner (Source: alliance-scs[.]org)*

Mitigations

- Recorded Future customers can use Brand Intelligence to track brand impersonations and typosquatting domains targeting their organization.
- Customers can use a Record Future query to track new domain registrations targeting maritime administrations mentioned in this report, including administrations in Benin, Bhutan, the Comoros, Chad, Malawi, Nicaragua, and Zambia.
- Customers can use a Record Future query to track AIS locations for vessels mentioned in this report (see Appendix B for the full list of vessel identifiers).
- Organizations in the maritime industry should incorporate threat intelligence workflows into due diligence checks to proactively identify fraudulent online infrastructure supporting SENs.
- Governments targeted by SENs should continue monitoring impersonations of their ship registries and maritime administrations.
- Governments targeted by SENs that also conduct multi-jurisdictional flag fraud should share information across organizations to enable appropriate legal and security responses.

Outlook

Online infrastructure, including websites and social media accounts, is very likely playing an increasingly important role in validating entities and corroborating documentation during port inspections and due diligence checks in the maritime industry. Consequently, SENs will very likely expand their use of cyber-enabled means to develop and maintain credible digital footprints, increasing the likelihood that fraudulent artifacts pass compliance checks. Online infrastructure also provides a layer of credibility that is likely easier to flexibly reconstitute than shell or front companies, allowing SENs to rapidly rotate identities in response to sanctions and enforcement actions.

Service providers underpinning the digital infrastructure will almost certainly remain financially incentivized to provide and iterate on capabilities and services to aid in sanctions evasion. Beyond operating inauthentic websites, they are likely to adopt generative artificial intelligence (AI) and synthetic identities to scale the production of fraudulent documents and enhance the credibility of their infrastructure.

Iranian and Russian shadow fleet operators will almost certainly continue using these service providers to evade sanctions and obfuscate their activity. Exposing these networks' online infrastructure should remain a priority for government officials and researchers in the maritime domain. However, these networks almost certainly aim to remain resilient in the face of takedowns with reusable website templates and infrastructure. Enforcement actions and sanctions should aim to target the underlying corporate entities and individuals, making attribution central to future investigations.

Appendix A: Indicators of Compromise (IoCs)

Domains

alliance-scs[.]org
atlasregister[.]net
atlasregister[.]org
benin-maritime[.]org
beninmaritime[.]bj
beninmaritime[.]co
beninmaritime[.]in
beninmaritime[.]net
beninmaritime[.]org
brunieshipclass[.]org
btn-shipreg[.]com
cameroonshipregistry[.]org
chad-maradmin[.]org
epnicaragua[.]com
epnicaragua[.]org
eqguinea-shipadmin[.]org
gove[.]bj
guve[.]bj
haiti-shipreg[.]com
hellasnaval[.]net
hss-registry[.]org
isithin[.]com
marinegov[.]org
medlloyd[.]online
medlloyd[.]org
mpabd-shipregistry[.]org
nauticacentro[.]com
nauticacentro[.]mx
niataregister[.]net
niataregister[.]org
pioneersmaritime[.]com
registry[.]zmgov[.]org
sasmaa[.]club
zambmaritime[.]org
zambshipadmin[.]org

Appendix B: Vessel Identifiers

Name	IMO	Sanctions
SOFIA K	9299123	Sanctioned in May 2025 by the UK — Russian shadow fleet
MAISAN	9289776	Sanctioned in April 2025 by the US — Iranian shadow fleet
STABILIS I	9234501	Sanctioned in May 2025 by the UK — Russian shadow fleet
OLAF I	9224465	Sanctioned in January 2025 by the US — Russian shadow fleet
BOLTARIS	9251456	Sanctioned in May 2025 by the UK — Russian shadow fleet
HANSON	9237412	Sanctioned in March 2025 by the US — Iranian shadow fleet
DIANCHI	9281011	Sanctioned in January 2025 by the US — Russian shadow fleet
BAISHA	9436941	Sanctioned in January 2025 by the US — Russian shadow fleet
SERENA	9255660	Sanctioned in December 2024 by the UK — Russian shadow fleet
MAKMUR	9078189	Entity of interest
TIS 520	9047300	Entity of interest
PRS OCEAN	9276561	Sanctioned in July 2025 by the UK — Russian shadow fleet
KATSUYA	9178068	Sanctioned in August 2025 by the US — Iranian shadow fleet
SERANO II	9165542	Entity of interest
GOLDEN LEO	9181833	N/A
JAMILA	9083275	N/A
BURAAQ	8914829	Entity of interest

Recorded Future reporting contains expressions of likelihood or probability consistent with US Intelligence Community Directive (ICD) 203: Analytic Standards (published January 2, 2015). Recorded Future reporting also uses confidence level standards employed by the US Intelligence Community to assess the quality and quantity of the source information supporting our analytic judgments.

About Insikt Group®

Recorded Future's Insikt Group, the company's threat research division, comprises analysts and security researchers with deep government, law enforcement, military, and intelligence agency experience. Their mission is to produce intelligence that reduces risk for customers, enables tangible outcomes, and prevents business disruption.

About Recorded Future®

Recorded Future is the world's largest intelligence company. The Recorded Future Intelligence Operations Platform provides the most complete coverage across adversaries, infrastructure, and targets. By combining precise, AI-driven analytics with the Intelligence Graph® populated by specialized threat data, Recorded Future enables cyber teams to see the complete picture, act with confidence, and get ahead of threats that matter before they impact your business. Headquartered in Boston with offices around the world, Recorded Future works with more than 1,900 businesses and government organizations across 80 countries.

Learn more at recordedfuture.com