Funded by the European Union

Endorsed by the 30th ASWGFi Meeting, 22-23 June 2022

Environment & Climate Change

Fisheries

Development of guidelines for sharing, access to, and use of IUU fishing-related information for the AN-IUU interactive platform

GUIDELINES ON SHARING, ACCESS TO AND USE OF IUU FISHING RELATED INFORMATION

Enhanced Regional EU-ASEAN Dialogue Instrument

E-READI

Disclaimer

This study is financed by the "Enhanced Regional EU-ASEAN Dialogue Instrument" (E-READI) a development cooperation program funded by the European Union. E-READI facilitates dialogues between the EU and ASEAN in priority policy areas of joint interest.

Mission of the European Union to ASEAN

Menara Astra, 38th Floor
Jl. Jend Sudirman Kav 5-6
Jakarta 10220, Indonesia
+62 (21) 2554 6200
mission-asean@eeas.europa.eu
MISSION-ASEAN-EREADI-CONCEPTS@eeas.europa.eu

ASEAN Secretariat

70A Jl. Sisingamangaraja
Jakarta 12110, Indonesia
+62 (21) 726 2991
ereadi@asean.org

This study is prepared by Seán P Marriott, Senior Non-Key Expert for Fisheries Information

1 Table of Contents

Table of Figures

List of Acronyms

Acronym	Meaning
AIS	Automatic Identification System
APFIC	Asia-Pacific Fisheries Commission
AMS	ASEAN Member States
AN-IUU	ASEAN Network for Combating IUU Fishing
ASEAN	Association of South-East Asian Nations
ASEAN-SEC	ASEAN Secretariat
ASWGFi	ASEAN Sectoral Working Group on Fisheries
CCALMR	Convention On The Conservation Of Antarctic Marine Living Resources
CCM	(Fisheries) Conservation And Management Measure
CCSBT	Commission for the Conservation of Southern Bluefin Tuna
CDS	Catch Documentation Scheme
EC	European Community/ Commission
EEZ	Exclusive Economic Zone
EU	European Union
FAO	Food and Agriculture Organisation [of the United Nations]
FAD	Fish Aggregating Device
FFA	(South Pacific) Forum Fisheries Agency
FOC	Flag of Convenience
FSA	[United Nations] Fish Stocks Agreement
FV	Fishing Vessel
FFV	Foreign Fishing Vessel
GT	Gross Tonnage
ICCAT	International Convention for the Conservation of Atlantic Tunas
ILM	International Legal Materials
ILO	International Labour Organisation
IMO	International Maritime Organisation
IOTC	Indian Ocean Tuna Commission
IPOA	International Plan of Action
IPOA-IUU	(FAO) International Plan of Action against IUU
IRCS	International Radio Call Sign
ITLOS	International Tribunal for the Law of the Sea
IUU	Illegal, Unrecorded and Unregulated [fishing]

Km	Kilometre
LOA	Length Overall
MCS	Monitoring, Control and Surveillance
MS	Member State
nm	Nautical Mile
PNG	[Independent State of] Papua New Guinea
PSM	Port State Measures
PSMA	Port States Measures Agreement
RFB	Regional Fisheries Body
RFMO	Regional Fisheries Management Organisation
RFVR	Regional Fishing Vessels Record
RPOA	Regional Plan of Action on Promoting Sustainable Fisheries including Combating IUU Fishing
RAN	Royal Australian Navy
SEAFDEC	Southeast Asian Fisheries Development Center
SOM-AMAF	Senior Officials Meeting of the ASEAN Ministers on Agriculture and Forestry
SWIOFC	South West Indian Ocean Fishery Commission
TDS	Trade Documentation Scheme
UN	United Nations
UNCLOS	1982 United Nations Convention on the Law of the Sea
UNODC	United Nations Office on Drugs and Crime
UNTS	United Nations Treaty Series
USA	United States of America
VMS	Vessel Monitoring System
WCPFC	Western & Central Pacific Fisheries Commission

Executive Summary

The Guidelines are an amplification of the initial Zero Draft, prepared by the AN-IUU. The enlarged Guidelines laydown a set of Guiding Principles

I. The National Focal Points for AN-IUU who are authorized to produce, share, and use data and metadata are stewards of those data, and have the responsibility for ensuring that the authenticity, quality, and integrity of the data are preserved, and to respect for the data source is maintained by ensuring privacy where appropriate";
II. Data should be labelled 'sensitive' or 'restricted' with appropriate justification and treated in accordance with the Principles for Sensitive Information-Handling, and should not be shared without due authorisation for use by the relevant AN-IUU Focal Points;
III. Data shall be handled and processed fairly and lawfully, under the legislation of the ASEAN Member State within which that data is collected, processed or passed on to the ASEAN IUU Network;
IV. Data shall not be transferred outside the ASEAN-IUU Network without adequate protection and authorisation from the AN – IUU Focal Point;
V. Data shall not be used for any purpose which is contrary to international law;
VI. Each focal point or identified national liaison point of the AN-IUU shall only share data to the extent allowed under its own national legislation for data privacy;
VII. Personal data shall not be shared within this network, and any data relating to any person shall be anonymised, where possible;
VIII. Data shall be checked for accuracy, and any data which is assessed as being inaccurate or liable to create harm, contrary to law, shall not be shared;
IX. Data shall be kept secure and handled in accordance with the Principles for Cyber-security[1]; and
X. Data shared within this network shall be only be used to meet the Purposes (of these Guidelines, as given above) and for no other purpose.

Acknowledgements

The consultant wishes to acknowledge the assistance of the AMS Focal Points within each of the States and who responded not only to his questionnaire but who also provided useful Information. In this regard, the advice and assistance of Thailand has been of particular value.

Particular thanks are also due to the E-READI Team Leader, Aldo dell'Ariccia, and to Joseph Arbiol, of the ASEAN Secretariat, who so carefully proofread the original document and corrected all the numerous typos and other infelicities. Thank you very much for a far better job than I would have done.

The consultant also wishes to record his appreciation of the valuable work done by "Stop Illegal Fishing" and the development of its inspectors' training, and training manuals, which have been a useful source of reference material.

[1] See Section 7

Thanks are also due to Professor Richard Barnes and the University of Lincoln for allowing the consultant time out to carry out this assignment.

1 Introduction to the Guidelines

This document is a guide for implementing the Information Sharing Principles under the framework of the ASEAN AN-IUU Network to combat IUU fishing. It outlines the procedures to be followed and identifies the common information sharing principles, which will be applied within the AN-IUU Network.

1.1 Brief history on the establishment of the AN-IUU network

Southeast Asia is among the world's top producers of fish and fishery products. In 2018, the Southeast Asian region contributed approximately 22 percent of the world's total fish production. The uptrend has been significant with the region's production of marine fisheries increasing from 33.6 million metric tons in 2011 to 46.0 million metric tons (MT) in 2018, of which just over 18 million MT was from marine fisheries.[2] In terms of the number of fishing vessels, more than 850,000 fishing vessels were operating in the ASEAN region in 2015 (SEAFDEC Website, 2015).

Given the interconnected and vast regional waters of ASEAN – nearly 13 million square kilometres - and the global nature of the fishery industry and the organized networks of criminals in the fishery sector, no one country can successfully tackle these challenges alone. A regional network approach is needed to better address the challenges faced and provide a formal basis for the sharing of information and coordination.

1.2 Purpose of the network

The ASEAN Network for Combating IUU Fishing will create a platform for both effective information sharing and an operational network that enables easy and effective communication among national authorities. The information-sharing should focus on enforcing national laws and regulations of the respective countries, as well as meeting international legal obligations. The Network may also assess where support and capacity building may be needed regionally.

Offences committed in the fisheries sector can be transnational in nature, which means that the illicit fishing activity of the vessel or any other illegal activity perpetrated by the vessel's managers or crew (e.g., forced labour, tax evasion or trafficking in drugs) is often subject to multiple jurisdictions.[3]

The transnational aspect of fisheries crimes can derive from various elements such as:

- the flag State of the fishing vessel;
- the coastal State in whose waters the fisheries crimes occurred;
- the port State where the illegal catches are landed;
- the nationality of individuals, operators and companies;
- the import or export State.[4]

[2] SEADEC 2019 fishery statistics http://map.seafdec.org/NewBulletin/index.php
[3] Interpol, *International Law Enforcement Cooperation in the Fisheries Sector* (Interpol 2018).
[4] International Law Enforcement Cooperation in the Fisheries Sector - INTERPOL

This multiplicity of jurisdictions results in the need for effective cooperation at the prevention, investigation and prosecution stages between the different AMS countries and administrations involved in order to work together to share information and connect investigations. Additionally, AMS have the option of transferring criminal proceedings from one country to another to increase the successful chances of a prosecution.[5]

2 Terms and definitions

Interactive platform	Interactive Platform is a regional common tool that is practical and "ready to use" for the focal points in an intuitive and real-time manner for the purpose of *Request / Alert / Share / Receive Information.*
AN – IUU Focal Point	Designated National Focal Point in each AMS
Network	Means the AN-IUU Network (the ASEAN Network for Combating IUU Fishing)
Warning/Alert	Notifications for warning or alert the ASEAN Member States (AMS) for tracking, monitoring or surveillance of the behaviour of fishing vessel which shall include but not limited to the fishing vessel (s) in the IUU Vessel List or the vessel that having a good reason to believe that it has violated the laws and regulations of Coastal State of the ASEAN Member States (AMS) or finding on non-compliance the conservation and management measures (CMMs) in the high seas or in the RFMOs areas or having suspicious behaviours to conduct IUU fishing or having been involved in IUU fishing or suspicious of IUU activities where ever the incident (s) occurs, etc.

3 Legal framework

1. United Convention on the Law of the Sea (UNCLOS);
2. United Nations Fish Stocks Agreement (UNFSA)
3. FAO Compliance Agreement
4. Port State Measures Agreement (PSMA)
5. FAO Code of Conduct for Responsible Fisheries
6. International Plan of Action to Prevent, Deter and Eliminate Illegal, Unreported and Unregulated Fishing (IPOA-IUU)
7. The Strategic Plan of Action on ASEAN Cooperation on Fisheries (2021 – 2025), and the Joint ASEAN- SEAFDEC Declaration on Regional Cooperation for Combating Illegal Unreported and Unregulated (IUU) Fishing
8. International Maritime Organization (IMO)
9. Regional Plan of Action to Prevent, Deter and Eliminate Illegal, Unreported and Unregulated (IUU) Fishing (RPOA-IUU)

[5] Interpol (n 1).

10. Sub-Regional Fisheries Agreements;
11. National Laws and Regulations.
12. Resolution and Plan of Action on Sustainable Fisheries for Food Security for the ASEAN Region Towards 2030

In addition, the following international instruments:

[ILO] C188 - *Work in Fishing Convention*, 2007 (No. 188)

2012 *Cape Town Agreement* (Cape Town Agreement On The Implementation Of The Provisions Of The 1993 Torremolinos Protocol Relating To The 1977 International Convention For The Safety Of Fishing Vessels)

4 Principles for an AN-IUU Information Sharing Arrangement

4.1 Basic Principles

This Section presents the policies and intent of the Guiding and Operational Principles for data-sharing, made under the *Cooperation Framework on ASEAN Network For Combating Illegal, Unreported, Unregulated (IUU) Fishing, of 28th July* 2020 (Cooperation Framework for IUU), and is intended to meet the above Declaration and Guiding and Operational principles by:

a) Creating the basis for sharing data on IUU fishing and activities which contribute to combatting IUU fishing both within the Region and outside it to the extent deemed appropriate to achieving the above Intent;
b) Providing support to fisheries and enforcement agencies within the Region to assist in combatting IUU fishing;
c) Assisting with the prosecution of IUU offenders by providing evidence of IUU-related activities from the resources of the ASEAN Network against IUU fishing, combined, where appropriate, with the assistance of the relevant agencies of ASEAN Member States.

4.2 Guiding Principles

Data relating to IUU-information shall be shared within the AN-IUU Network in accordance with the following principles:

XI. The National Focal Points for AN-IUU who are authorized to produce, share, and use data and metadata are stewards of those data and have the responsibility for ensuring that the authenticity, quality, and integrity of the data are preserved, and to respect for the data source is maintained by ensuring privacy where appropriate";
XII. Data should be labelled 'sensitive' or 'restricted' with appropriate justification and treated in accordance with the Principles for Sensitive Information-Handling, and should not be shared without due authorisation for use by the relevant AN-IUU Focal Points;
XIII. Data shall be handled and processed fairly and lawfully, under the legislation of the ASEAN Member State within which that data is collected, processed or passed on to the ASEAN IUU Network;
XIV. Data shall not be transferred outside the ASEAN-IUU Network without adequate protection and authorisation from the AN – IUU Focal Point;
XV. Data shall not be used for any purpose which is contrary to international law;
XVI. Each focal point or identified national liaison point of the AN-IUU shall only share data to the extent allowed under its own national legislation for data privacy;

XVII. Personal data shall not be shared within this network, and any data relating to any person shall be anonymised, where possible;

XVIII. Data shall be checked for accuracy, and any data which is assessed as being inaccurate or liable to create harm, contrary to law, shall not be shared;

XIX. Data shall be kept secure and handled in accordance with the Principles for Cyber-security[6]; and

XX. Data shared within this network shall be only be used to meet the Purposes (of these Guidelines, as given above) and for no other purpose.

The Guidelines document amplifies the above principles and, provides clarification concerning international law relating to IUU fishing and the arrest of vessels.

4.3 Information sharing should follow the STARR Principles

The STARR principles provide a useful guide for how and what information to share. The most important consideration is whether sharing information is likely to combat IUU fishing in the ASEAN and assist international efforts to combat IUU Fishing globally.

- **SECURE** - Information must be shared and stored securely according to AN-IUU network requirements.
- **TIMELY** - Timeliness is particularly important in addressing and combatting IUU fishing.
- **ACCURATE** - Accurate and up to date information is vital and should clearly distinguish between facts and opinion.
- **RELEVANT** - Only information relevant and appropriate to the purpose should be shared with those who need it. The information shared must not include unnecessary detail and must be directly relevant to the purpose of combatting IUU Fishing
- **RECORD** - Information sharing decisions should be recorded, such as what information has been shared and with whom and for what purpose. If the decision was made not to share information, it is also good practice to record this decision.

5 Clarification on the definition of Illegal, Unreported and Unregulated Fishing

5.1 The FAO Definitions

The definition of IUU fishing is given in the 2001 *FAO International Plan of Action to Prevent, Deter and Eliminate Illegal, Unreported and Unregulated Fishing* (IPOA-IUU). The definitions of IUU are given in Part II (paragraph 3)[7] these definitions have remained unchanged – and were transposed into other legislation, notably in the EU IUU Regulation (Regulation 1005/2008[8]). The definitions are given below;

5.2 The original definitions

"3.1 Illegal fishing refers to activities:

[6] See Section 8

[7] FAO, *International Plan of Action to Prevent, Deter and Eliminate Illegal, Unreported and Unregulated Fishing.* (FAO 2001).{IPOA-IUU)

[8] Council Regulation (EC) No 1005/2008 of 29 September 2008 establishing a Community system to prevent, deter and eliminate illegal, unreported and unregulated fishing. OJ L 286/1 [2008]

3.1.1 conducted by national or foreign vessels in waters under the jurisdiction of a State, without the permission of that State, or in contravention of its laws and regulations;

3.1.2 conducted by vessels flying the flag of States that are parties to a relevant regional fisheries management organization but operate in contravention of the conservation and management measures adopted by that organization and by which the States are bound, or relevant provisions of the applicable international law; or

3.1.3 in violation of national laws or international obligations, including those undertaken by cooperating States to a relevant regional fisheries management organization.

3.2 Unreported fishing refers to fishing activities:

3.2.1 which have not been reported, or have been misreported, to the relevant national authority, in contravention of national laws and regulations; or

3.2.2 undertaken in the area of competence of a relevant regional fisheries management organization which have not been reported or have been misreported, in contravention of the reporting procedures of that organization.

3.3 Unregulated fishing refers to fishing activities:

3.3.1 in the area of application of a relevant regional fisheries management organization that is conducted by vessels without nationality, or by those flying the flag of a State not party to that organization, or by a fishing entity, in a manner that is not consistent with or contravenes the conservation and management measures of that organization; or

3.3.2 in areas or for fish stocks in relation to which there are no applicable conservation or management measures and where such fishing activities are conducted in a manner inconsistent with State responsibilities for the conservation of living marine resources under international law."

5.3 Interpreting the definitions

What these definitions cover in practice is illustrated in the different types of IUU fishing in different waters. The range of waters goes from inland (freshwater) to areas of the high seas beyond national jurisdiction. **Error! Not a valid bookmark self-reference.** illustrates the different types of IUU fishing in different waters. It also includes areas under the authority of an international convention - the area of a Regional Fisheries Management Organisation (RFMO) as a body which sets its own Control and Conservation (management Measures (CCMs).

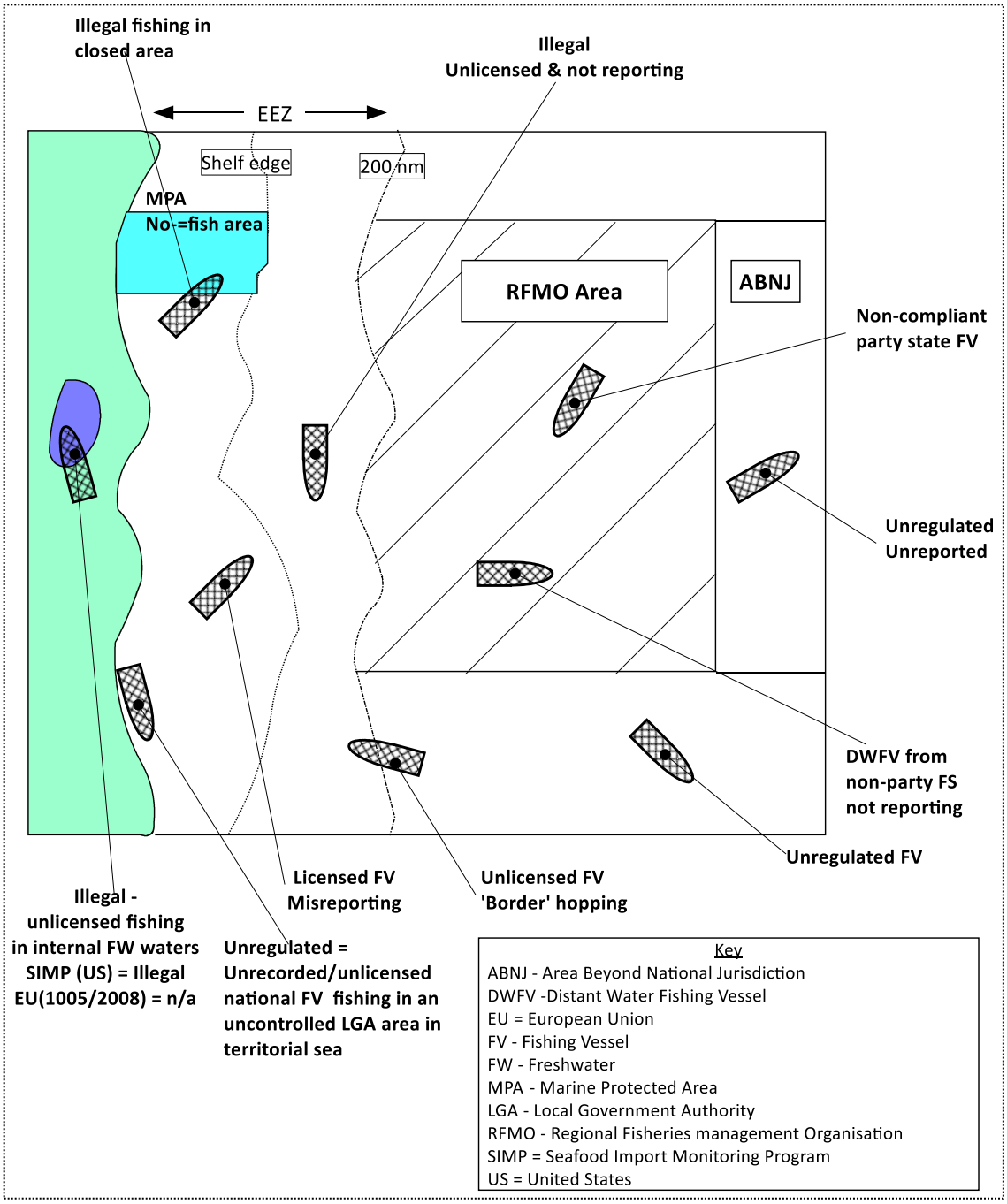


Figure 1. Types of IUU Activities

Reading the text of the IPOA-IUU more closely, the term 'Illegal ' fishing is reasonably obvious but 'Unreported'(fishing) is perhaps less clear; nevertheless, it is important in that both *not* reporting or *mis*-reporting (i.e. making a false or erroneous report) are covered, again in both national and RFMO waters. 'Unregulated' fishing is perhaps more complex in that it refers to fishing within an RFMO area carried out by:

> "…by vessels without nationality, or by those flying the flag of a State not party to that organization, or by a fishing entity, in a manner that is not consistent with or contravenes the conservation and management measures of that organization…"[9]

Para. 3.3.2 makes it clear that 'Unregulated' fishing also includes fishing in "in areas or for fish stocks" where there are "no applicable conservation or management measures" and that such activities are "inconsistent" with the State's responsibilities to conserve stocks in accordance with international law. This has direct application to failures in national governments' management of fisheries. For example, where a state fails to properly record or register its fishing vessels, or where in an area, not directly controlled by central government, where the local administrative authority does not properly regulate the local fishery, then these situations create unregulated fisheries. For central government, failing to ensure its fish exports are identified as not being of IUU origin, or products from unregulated fisheries, poses a risk of damaging its export trade.

The major departure between the FAO definitions and the EU definition is that the EU legislation is directed at marine fisheries, indeed specifically excepting freshwater fishery products. The FAO definition of illegal fishing defines it as

> "…activities…in waters under the jurisdiction of a State, without the permission of that State…"[10]

meaning that freshwater fisheries are included, as in misreporting (Unreported). The definition of Unregulated fisheries would appear to be ambiguous since, under para. 3.3.1 of the IPOA-IUU, the reference is to the "area of application of a relevant regional fisheries management organization" which could be understood to also include specifically inland RFMOs, such as CACFish,[11] although para.33.2 clearly refers to "living marine resources".

IUU fishing has become a shorthand term for a particular type of deliberate non-compliant fishing The important point that needs to be understood is that IUU fishing is not solely carried out by dedicated, criminal fishing vessels; the definition includes all fishing activities where fish are taken illegally, or where skippers fail to report, or deliberately falsify catch returns, or where national governments fail to provide proper governance of the resources under their control. However, owners (and co-operating skippers) that are deliberately non-compliant (IUU), choose to operate their business as 'criminal' or near criminal enterprises

[9] Para. 3.3.1 of the IPOA-IUU FAO (n 4).
[10] FAO. IUU-IPOA, para.3.1.1
[11] Central Asian and Caucasus Regional Fisheries and Aquaculture Commission

5.4 The definitions in international law practice

It has to be understood that the FAO IPOA-IUU definitions are themselves only guidelines. The FAO IPOA-IUU was intended to act as the basis for each country to create its own National Plan of Action (NPOA) with its own rules. Thus, the actual definitions which apply to the control of IUU fishing are the definitions of Illegal, Unreported and Unregulated, as they are defined in relevant national legislation or as they are defined in the resolutions and CCMs of the RFMOs. It is these definitions, not the FAO definitions, that determine whether or not a fishing vessel is declared to be "IUU fishing". This is an important point which needs to be understood.

Since 2001, there have been no further clarifications by FAO, of the meaning of IUU. Consequently, the international law definition of IUU is as given in the IPOA-IUU.[12] However, the later 2009 Port States' Measures Agreement[13] (PSMA) defines "IUU" as having the meaning given in the IPOA-IUU,[14] Recognising that the Guidelines should operate within established international law, the PSMA definitions offer scope for achieving greater exactitude for interpreting IUU in practical terms.

"Article 1

Use of terms

(a) "conservation and management measures" means measures to conserve and manage living marine resources that are adopted and applied consistently with the relevant rules of international law including those reflected in the Convention;

(b) "fish" means all species of living marine resources, whether processed or not;

(c) "fishing" means searching for, attracting, locating, catching, taking or harvesting fish or any activity which can reasonably be expected to result in the attracting, locating, catching, taking or harvesting of fish;

(d) "fishing related activities" means any operation in support of, or in preparation for, fishing, including the landing, packaging, processing, transhipping or transporting of fish that have not been previously landed at a port, as well as the provisioning of personnel, fuel, gear and other supplies at sea;

(j) "vessel" means any vessel, ship of another type or boat used for, equipped to be used for, or intended to be used for, fishing or fishing related activities.

5.5 Definitions in RFMO practice

The IOTC CCMs define IUU fishing within its area for the purpose of identifying an offending vessel as "IUU" and thus capable of being listed as such on the IOTC IUU Vessel List. The definitions are given below so that they can be compared with both the IPOA-IUU and the PSMA definitions.

[12] Par. 3.1 – 3.3
[13] Agreement on Port State Measures to Prevent, Deter and Eliminate Illegal, Unreported and Unregulated Fishing, 2009. 55 ILM 1157 (2016).
[14] PSMA, Art. 1 (e)

Definition of IUU Fishing Activities[15]

4. For the purposes of this Resolution a vessel is presumed to have engaged in IUU fishing activities when a Contracting Party or Cooperating Non-Contracting Party (hereinafter referred to as "CPCs") has provided information that such a vessel has, within the IOTC Area and in relation to species covered by the IOTC Agreement or by IOTC Conservation and Management Measures:

a) engaged in fishing or fishing-related activities and is neither registered on the IOTC Record

of Authorised Vessels in accordance with Resolution 15/04, nor recorded in the Active list of vessels; or

b) engaged in fishing or fishing related activities when its flag State is without quota, catch limit, or effort allocation under IOTC Conservation and Management Measures where applicable unless that vessel is flagged to a CPC ; or

c) failed to record or report its catches in accordance with IOTC Conservation and Management Measures or has made false reports; or

d) taken or landed undersized fish in contravention of IOTC Conservation and Management

Measures; or

e) engaged in fishing or fishing related activities during closed fishing periods or in closed areas in contravention of IOTC Conservation and Management Measures; or

f) used prohibited fishing gear in contravention of IOTC Conservation and Management Measures; or

g) transhipped fish to, or otherwise participated in joint operations with, support or re-supply vessels that are not included on the IOTC Record of Authorised Vessels or not on the Record of Vessels Authorised to Receive Transhipments At-Sea in the IOTC Area; or

h) engaged in fishing or fishing related activities in waters that are under the national jurisdiction of a coastal State without the permission or authorisation of that State or in contravention of the laws and regulations of that State (without prejudice to the sovereign rights of the State concerned to undertake enforcement measures against such a vessel)1; or

i) engaged in fishing or fishing related activities whilst being without nationality; or

j) engaged in fishing or fishing related activities having intentionally falsified or concealed its markings, identity or registration; or

k) engaged in fishing or fishing related activities in contravention of any other binding IOTC Conservation and Management Measures,

The key points to note are the inclusion of support vessels within the ambit of IUU vessels and that under sub-article (j) concealing or falsifying the markings on a fishing vessel creates the presumption that the vessel is engaged in IUU fishing operations.

5.6 Examination of IUU Definitions for state practice

Based on the above developments in international law, and in state practice within the ASEAN region the following clarifications can assist with definitions in national legislation:

[15] IOTC Resolution 18/03 On Establishing a List of Vessels Presumed to Have Carried out Illegal, Unreported and Unregulated Fishing in the IOTC Area of Competence. Date of Application: 4th October, 2018

"Fish" therefore includes all fish, piscine or otherwise products, in any stage of condition, including processed products. As such they are capable of being inspected to determine their legality or if the capture, processing, transhipment and any other transiting, exchange or processing treatment involved any IUU-related activities .[16]

"Fishing" therefore includes any activity which may be directed towards the capture of "fish". As 'attracting' is included, this means that Fish Aggregating Devices' (FADs) come under the definition of fishing. This has substantial implications for the control of FADs, whether covered under national legislation or any Regional Fisheries Management Organisation (RFMO) Control and Conservation Measures (CCMs). A FAD which is unmarked or otherwise, unlinked to a specific fishing vessel, which drifts (dFAD – drifting FAD) into the EEZ of an ASEAN Member State (AMS), for which that vessel is not licensed, can therefore be treated as fishing legally, and not likewise reporting. The use of the term 'locating' means that the use of fish finders or other form of finder, including aircraft' capable of communicating to a fishing vessel where to find a school of fish. For prosecution purposes, such fish should be capable of being identified as a target species for that vessel. Having a fish-finder is not a "crime" in itself but the use of it to direct the placing of a vessel, such that it could be reasonably expected to make use of the locator information to capture such fish, would be included as "fishing."

"Fishing-related activities" therefore includes all activities related to processing, as well as transhipping, at sea or in port, and transporting. Thus, the carriage of IUU fish by air, sea or land would be included with the ambit of what could be inspected or prosecuted as a "related-activity"[17]. What should be noted is that "fishing-related activities" includes activities in support of fishing – provisions, carrying or transferring crew, fuel, gear and any other type of supply (which could include engine parts), This expansion of the definition of fishing-activity thus includes carrier and bunkering vessels, as well as aircraft which would then also include any form of drone which might be used for spotting tunas schooling around a FAD; FADS have been already identified as being used to attract fish[18].

"Inland fishing". The PSMA specifically refers to "living marine resources" which therefore excludes freshwater species (as with the EU-IUU Regulation[19]). However, the IPOA-IUU definition under paragraph 3.1.3 states:

> "in violation of national laws or international obligations, including those undertaken by cooperating States to a relevant regional fisheries management organization."

This argues that any fish, marine or freshwater, taken in contravention of national law can be classed as IUU. And treated as such. Freshwater fish would not however come within the ambit of port inspections, resulting in refusal of entry to a ship carrying freshwater IUU products of IUU origin,

"Vessel" therefore includes all ships acting in support (carriers and bunker vessels) of a fishing vessel. As regards FADs, it has been argued that a FAD does not have to be defined as a vessel, it is sufficient that it acts as an attractor of fish.[20]

---

[16] Meaning any change to the fresh whole product, including gutting, washing, chopping, pasteurising, freezing, fermenting, packaging and treatment with additives which might extend shelf life or appearance or taste.

[17] Provided that such fish has not been previously landed "at a port".

[18] "Attracting" would include such activities as 'baiting' toas part of tuna pole-and -line fishing.

[19] Council Regulation (EC) No 1005/2008 of 29 September 2008 establishing a Community system to prevent, deter and eliminate illegal, unreported and unregulated fishing. OJ L 286/1 [2008

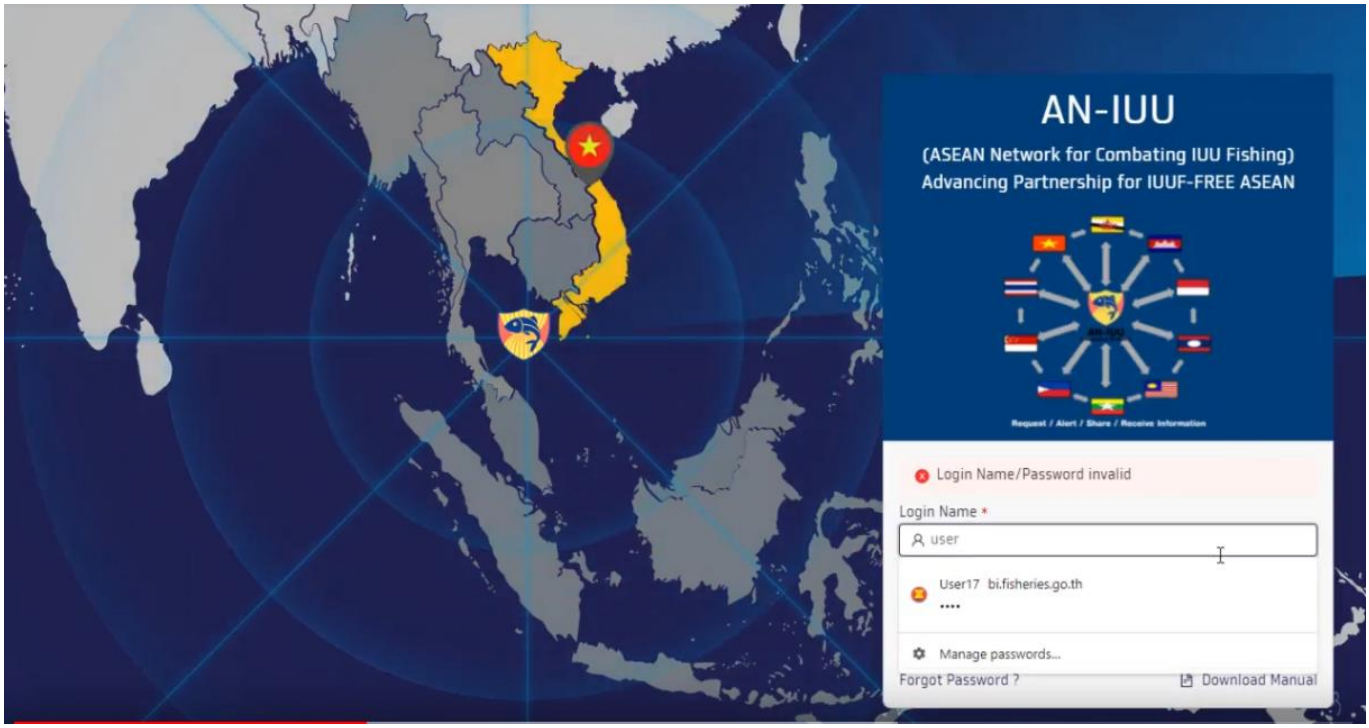
[20] Guillermo Gomez and others, 'The IUU Nature of FADs: Implications for Tuna Management and Markets' (2020) 48 Coastal Management 534 <https://doi.org/10.1080/08920753.2020.1845585>.

6 Using a platform for information-sharing

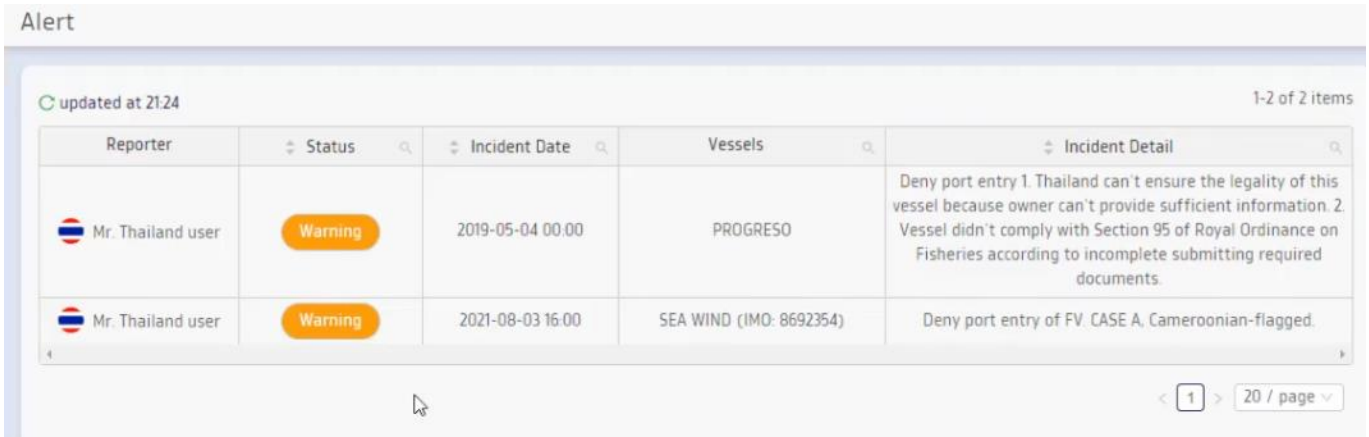
6.1 The AN-IUU Platform

The AN-IUU platform for -sharing information and has the merit of being developed and established within the region. The procedures to be followed are clear and relatively easy to use by competent staff and the data records provide a comprehensive record of reported vessels, including photographs and position data. .

6.2 Platform entry and incident reports

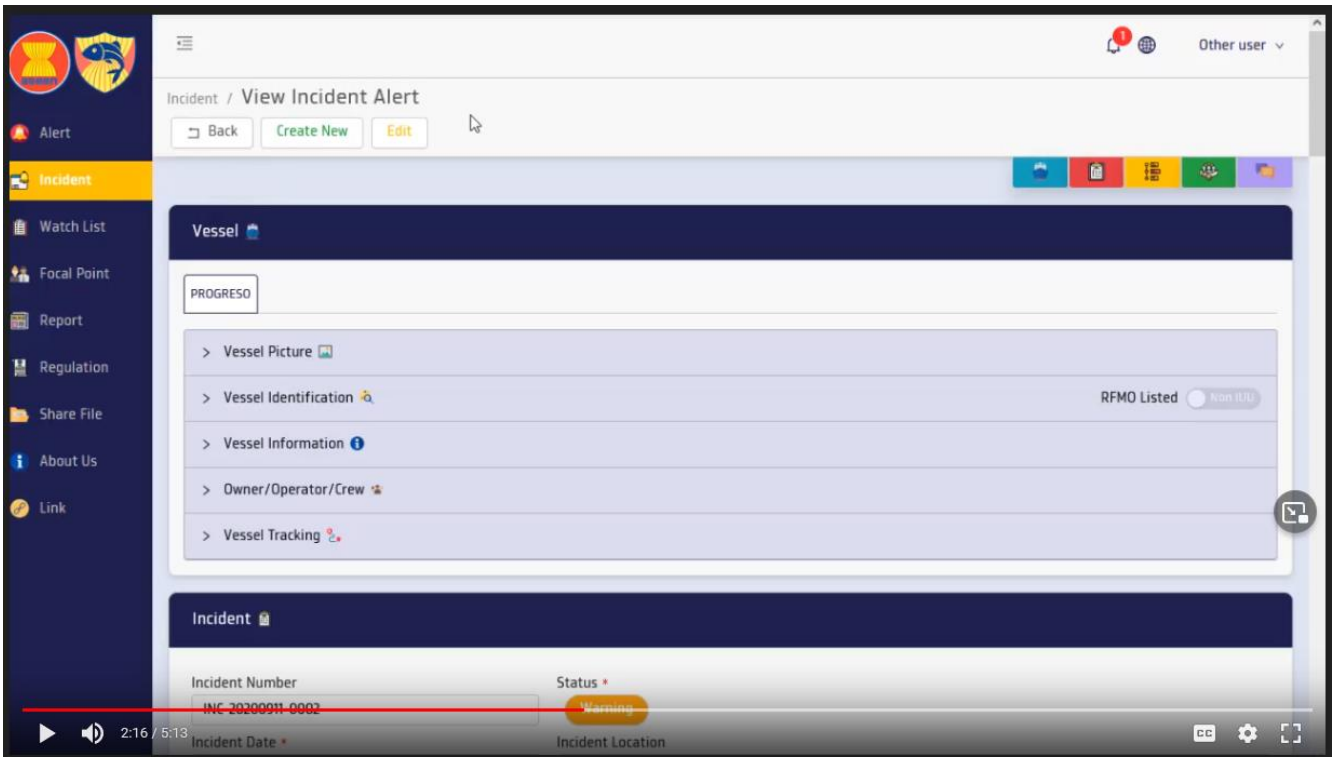


6.3 Incident report

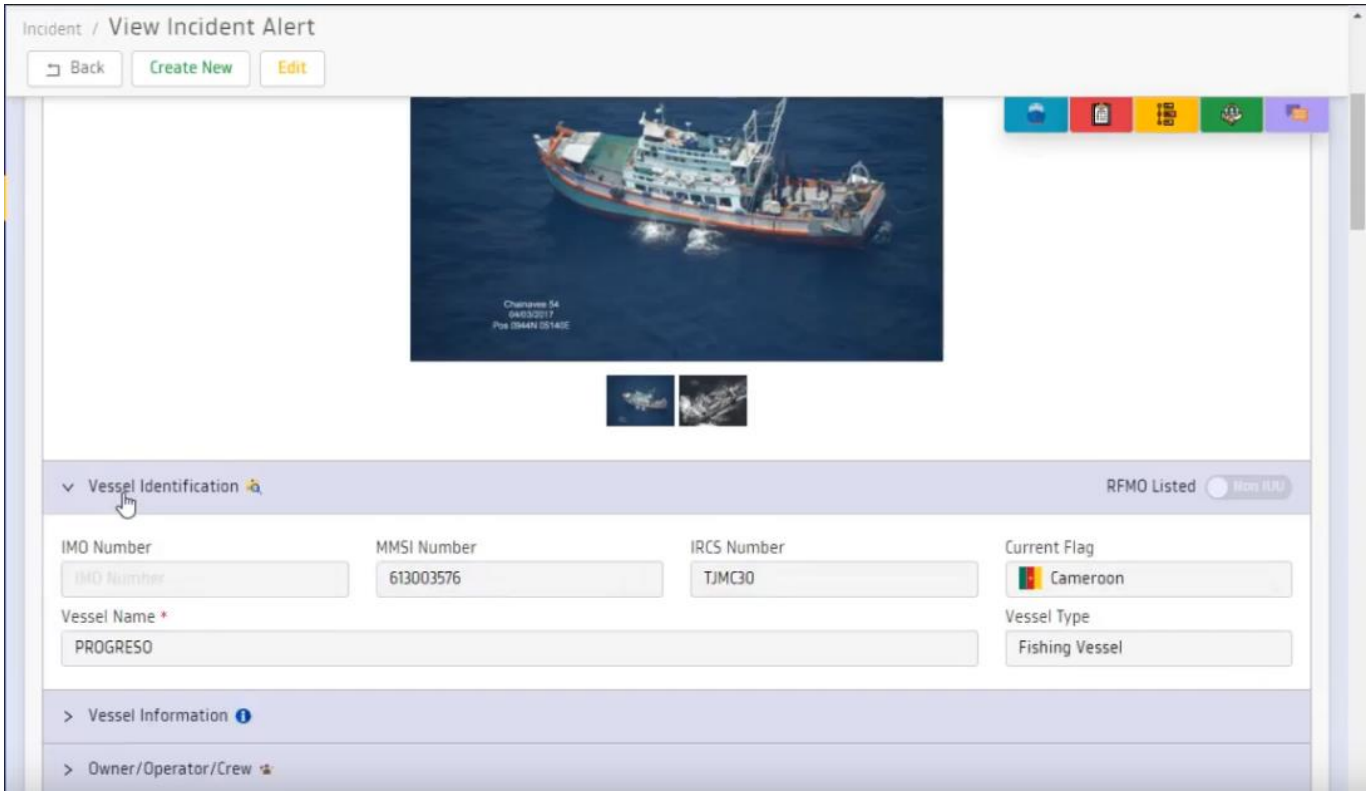


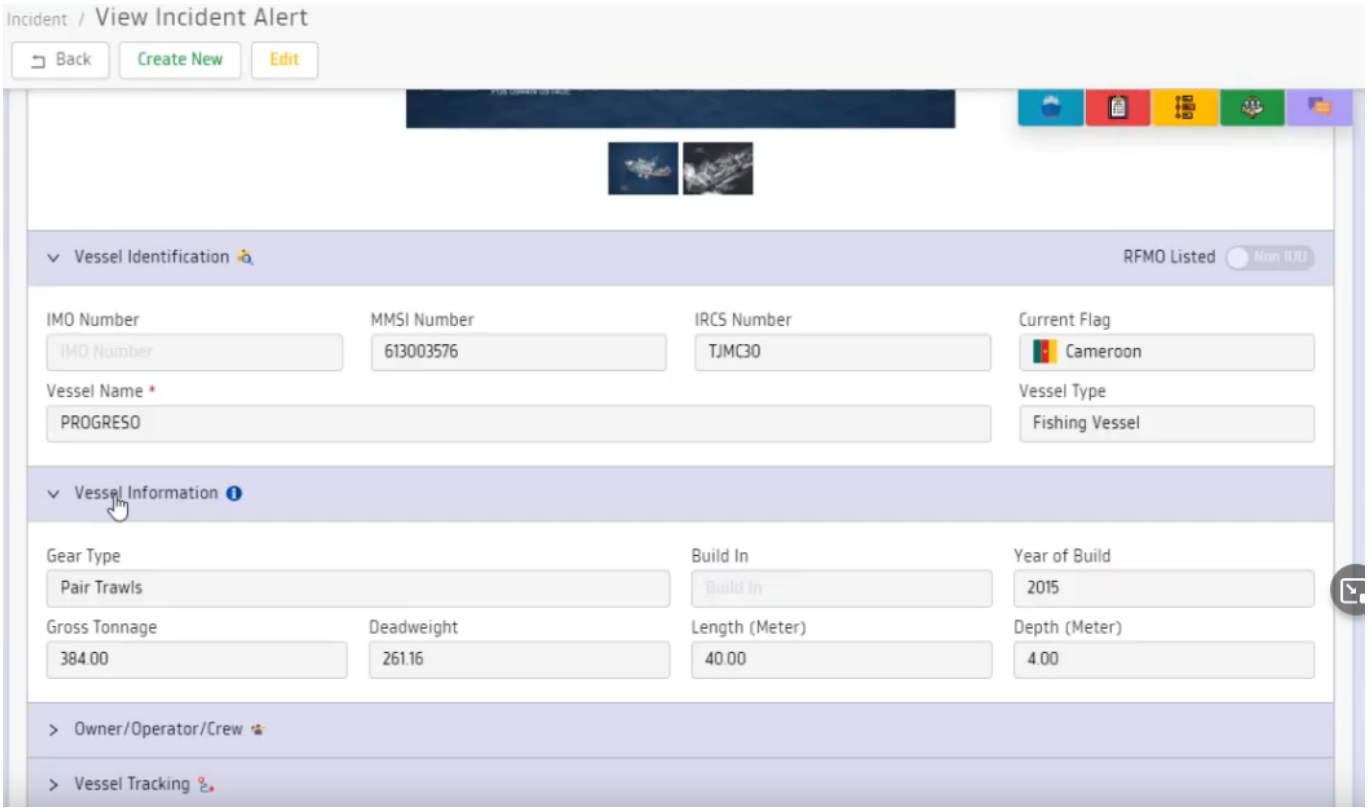
Following the entry point – log-on – the Incident reports can be seen. Above is shown a report by the Thai Focal Point, reporting a vessel with an alert status and an incident report itself.

Icons on the top right enable the user to access the sub-menus



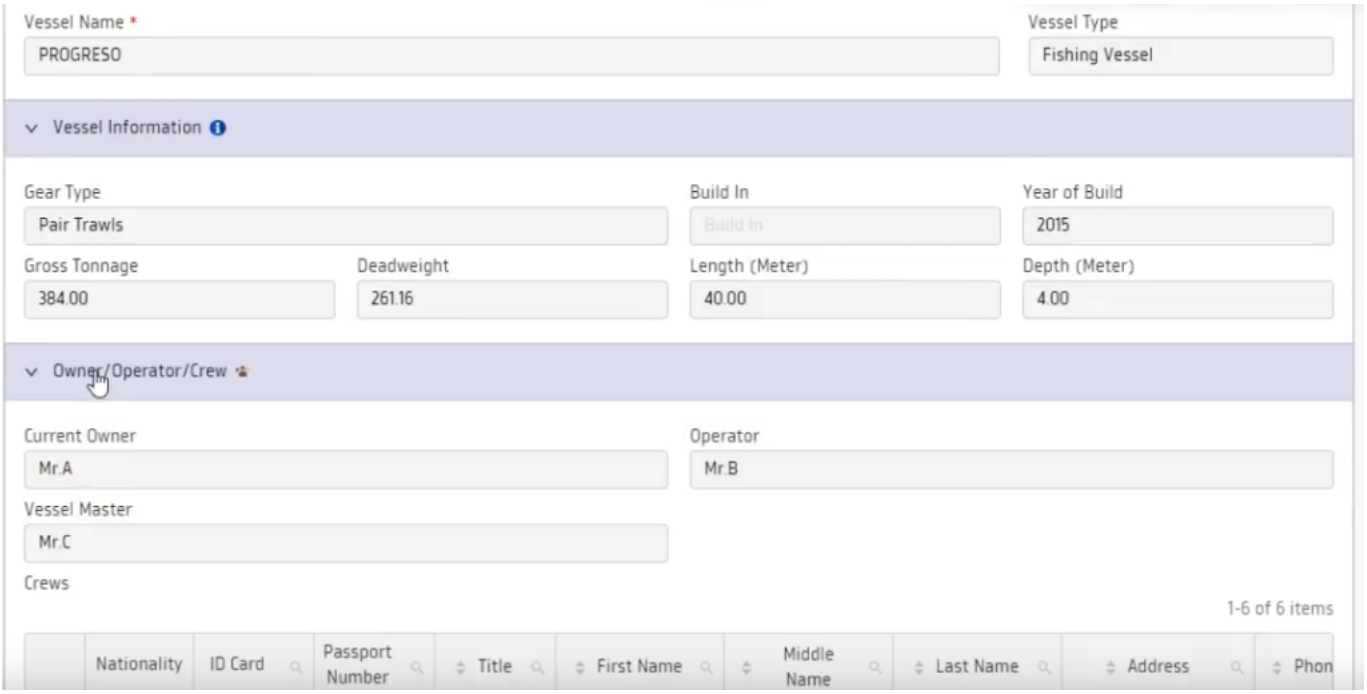
Working through the incident report menus enables the users to see a photograph of the vessel together with its details





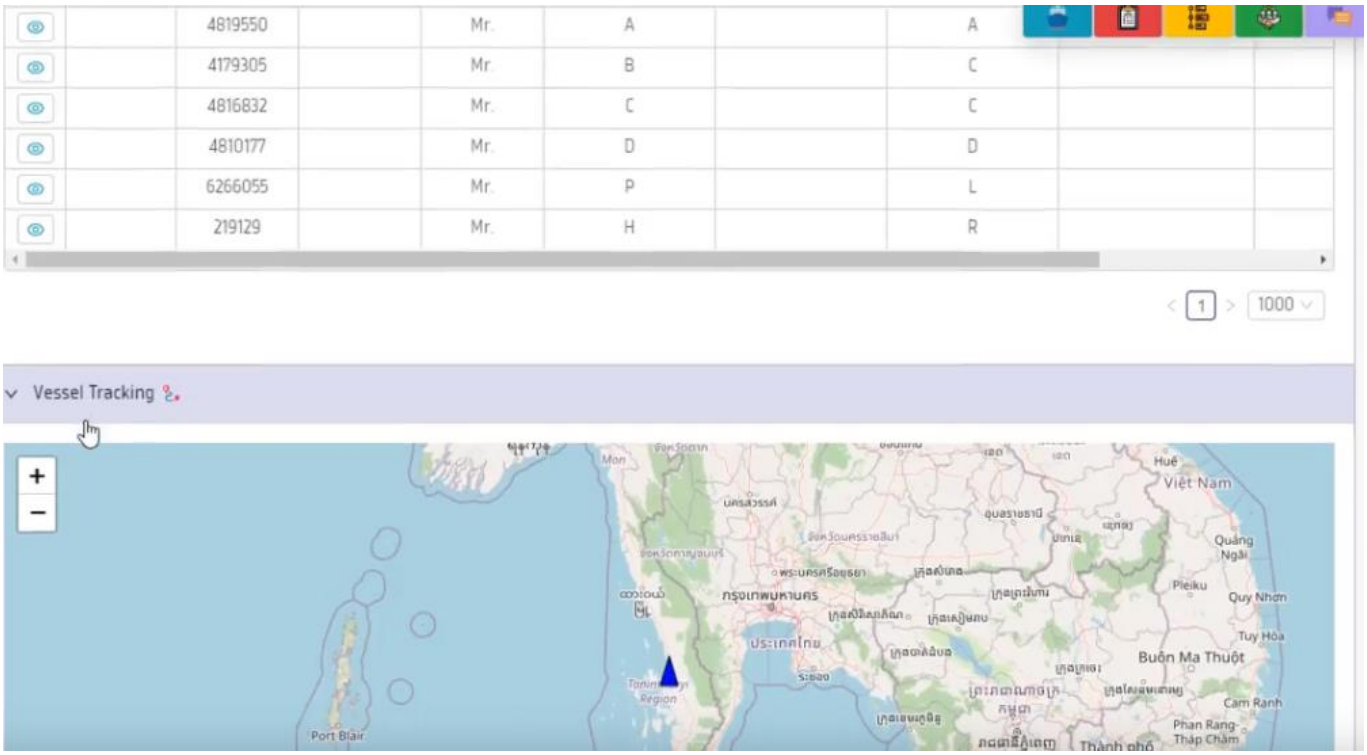
The incident details can be entered and seen by the user.

Together with owner/operator details

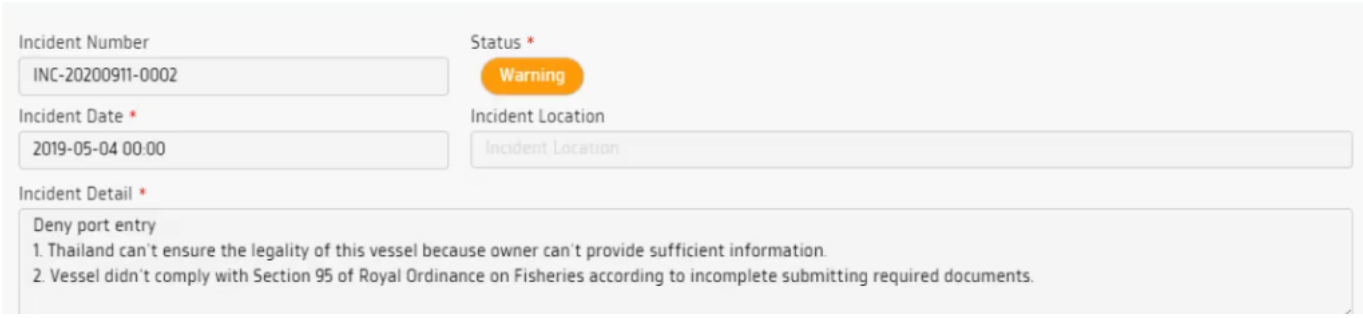


.

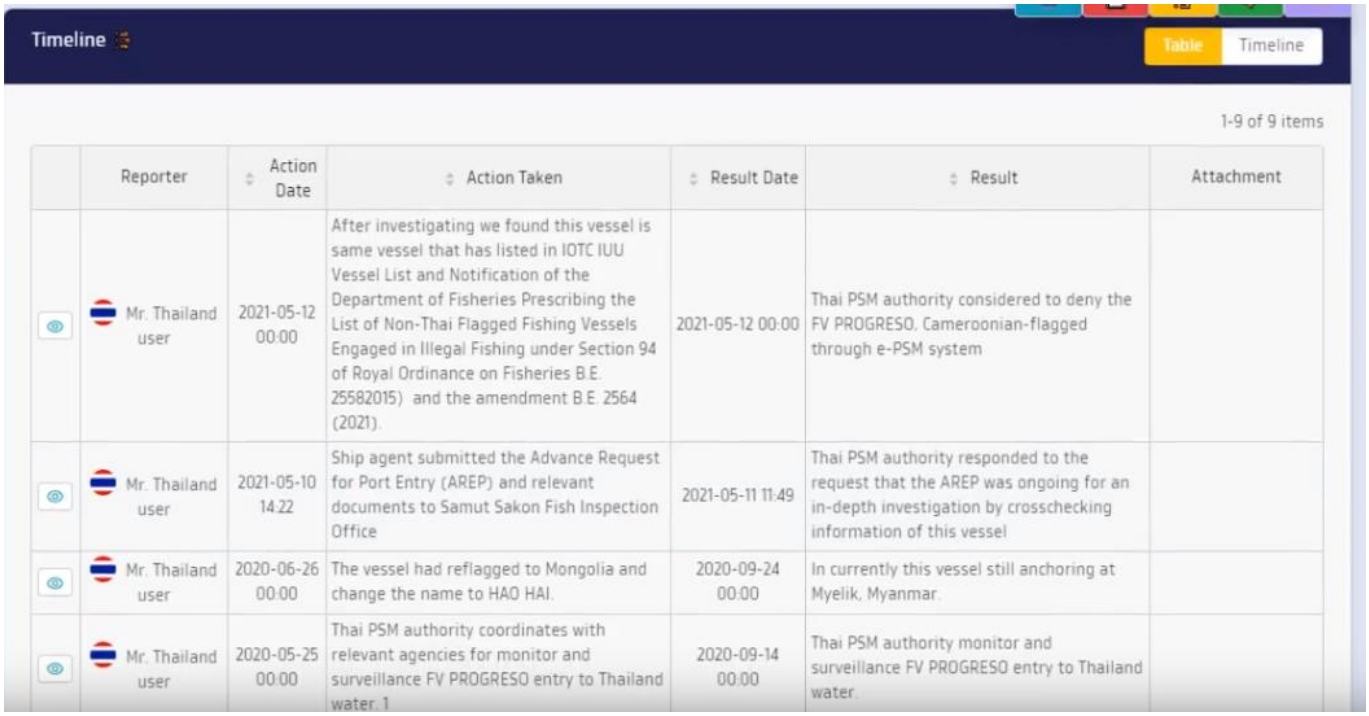
Position and tracking details- as visuals – can also be recorded and accessed.



An incident number is given with the date of the incident, together with details of the incident.



details of incident history can also be accessed with reference to the person reporting (see below)

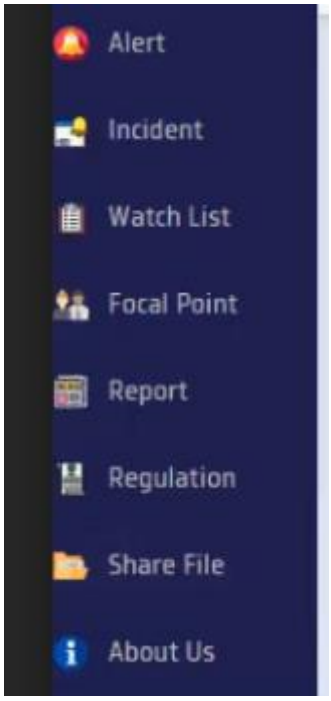


An interactive platform is available on the site which enables users to share information and to discuss incidents.

6.4 Watch List

The Watch list follows incident report and gives details of the vessels on the list

6.5 Additional information



The site provides additional information to users, enabling them to access information about the national focal points and to see reports from other countries of enforcement actions and other news information. The same menu allows users to see national regulations and to share files. Details of other watch lists from RFMOs can also be accessed.

6.6 Data Dictionary

The term ‘Data Dictionary’ is given to the data record of reported ships (as shown below):

6.7 Vessel details

AN-IUU Data Dictionary

1. Vessel

Vessel photographs

Picture	File	Colour photographs of the vessel recommended 3 photographs with at least 640x480 pixel each showing the whole structure; • The starboard side and portside of the vessel, • The bow of the vessel; • At least one of the photographs clearly showing at least one of the external markings specified in Name of vessel(s), and national register number(s) or as much as possible

Vessel identification

Vessel Name	Text	Vessel Name must be unique not duplicate. In case that reporter is not certainthat vessel is the same. User can add "#Number" after vessel name.
IMO Number	Text	IMO number
MMSI Number	Text	MMSI number
IRCS Number	Text	IRCS number
CurrentFlag	Select from lists	List of Countries
VesselType	Select from lists	Fishing Vessel or Carrier Vessel

Vessel information

GearType	Select from lists	Fishing Gear. To add more type of
Built in	Text	Shipyard, city or country that vessel was built
Year of Built	Text	Year that vessel was built e.g.,2560 B.E.
Gross Tonnage	Number	The volumeof all ship's enclosed spaces (from keel to funnel) measured to the outside of the hull framing.

Dead Weight	Number	The total weight of cargo, fuel, water, stores, passengers and crew and their effects that a ship can carry when at her designed full-load draft
Length (Meter)	Number	Length Overall vessel in meter
Depth (Meter)	Number	Depth of Vessel in meter
	Owner/Operation/Crew	
Current Owner	Text	A person having the ownership or the right to possession of a fishing vessel.
Operator	Text	Any person who is in charge or responsible of the operation or directive of control of a vessel, including the owner, charterer, master and the beneficiary of the economic or financial benefit of the vessel operation.
Vessel Master	Text	A person having command or charge of a fishing vessel or carrier vessel
	Crew	
ID Card	Number	Identification card; an official card or relevant document
Passport Number	Number	Passport Number
First Name	Text	Crew's First Name
Middle Name	Text	Crew's Middle Name
Last Name	Text	Crew's Last Name
Birth Date	Date	YYYY-MM-DD crew's birth date
Email	Text	Crew's Email
Nationality	Select from lists	List of Countries
Phone No.	Text	Crew's Phone Number
Mobile No.	Text	Crew's Mobile Number
Fax No.	Text	Crew's Fax Number
Address	Text	Crew's Address

6.8 Vessel tracking

Vessel Tracking

Time	Text	data timestamp AIS format –unix timestamp Human readable format – UTC
LATITUDE	Text	geographical latitude AIS format – in 1/10000 minute i.e., degrees multiplied by 600000 Human readable format – degrees
LONGITUDE	Text	geographical longitude AIS format – in 1/10000 minute i.e., degrees multiplied by 600000 Human readable format – degrees
Course Over Ground (degrees)	Text	Course Over Ground AIS format – in 1/10 degrees i.e., degrees multiplied by 10. COG=3600 means "not available" Human readable format – degrees. COG=360.0 means "not available"
Speed Over Ground (knots)	Text	Speed Over Ground AIS format – in 1/10 knots i.e., knots multiplied by 10. SOG=1024 means "not available" Human readable format – knots. SOG=102.4 means "not available"
HEADING	Text	current heading of the AIS vessel at the time of the last message value in degrees, HEADING=511 means "not available"
Position Accuracy	Text	(AIS format only) – Position Accuracy 0 – low accuracy 1 –high accuracy
Position Accuracy	Text	(AIS format only) - Rate of Turn
Navigational Status	Text	Navigational Status
IMO	Text	IMO ship identification number
NAME	Text	vessel's name (max.20 chars)
CALLSIGN	Text	vessel's callsign
Vessel Type	Text	vessel's type (more details here)
Position Device Type	Text	positioning device type (more details here)
Dimension to Bow	Text	Dimension to Bow (meters)
Dimension to Stern (meters)	Text	Dimension to Stern (meters)
Dimension to Port	Text	Dimension to Port (meters)

(meters)		
Dimension to Starboard (meters)	Text	Dimension to Starboard (meters)
DRAUGHT	Text	AIS format – In 1/10 meters i.e., draught multiplied by 10. Human readable format – meters
Destination	Text	vessel's destination
ETA	Text	Estimated Time of Arrival. Human readable format – UTC date/time

6.9 Incident report and timeline

2.Incident

Incident Number	Number	Generate automatically by system (running number)
Status	Select from lists	Overall rating of this incident depends on urgency or risk
Incident Date	Date	Dateand Timeof Incident
Incident Detail	Text	Detail of Incident.
Note	Text	Note about attachment
Attachments	File	Attach any file about incident

3.Timeline

Reporter	User	User who creates this timeline
Action Date	Date	YYYY-MM-DD HH:MM date of action
Action Taken	Text	Detail of Incident order by date e.g.,1. found vessel 2. incident led to suspect 3. detain vessel 4. found more evident or 5. capture
Result Date	Date	YYYY-MM-DD HH:MM date of result
Result Detail	Text	Detail of Incident order by date e.g.,1. found vessel 2. incident led to suspect 3. detain vessel 4. found more evident or5. capture

7 Procedures for sensitive information-handling

7.1 Introduction

All information relating to IUU fishing should be regarded as intelligence and must be treated as such.[21] That means that the intelligence report should be handled in a standard manner with a duty of care, combined with a careful assessment of the quality of the report. This assessment should also assess the sensitivity of the material, carrying out a risk assessment as to the source and the effect of how the intelligence will be made use of. In general, passing IUU information amongst other parties will help to defeat IUU abuse,[22] however, care should be taken to ensure that where the source may be at risk then that source should be protected. Information needs to be evaluated to determine its value – reliability – and the best use to be made of it. Best use also means an appreciation of the 'time-value' of information: the older information becomes, the less value it has. Weak information acted on immediately is more useful than good information used too late.

Information systems design and theory uses a **single source of truth** (SSOT) which is the basis for organising information and associated data so that every data element is maintained (mastered) in only one place. All other locations of the data must refer back to the primary "source of truth" location. Therefore, any updating of data element in the primary location must be able to also update the other information in the system without duplicating the information or for information to be lost, or otherwise forgotten. Information needs to be properly recorded and made easily accessible.

Good record-keeping means that research can be carried out, particularly in support of prosecutions. Research into information helps to build up a picture of illegal activity, helping to identify suspect vessels but also transhipments and bunkering operations. Such information improves patrolling and helps to make interception successful.

Information is a good tool in the battle against IUU and like all good tools, it must be treated with respect and used properly, and not wasted.

The following principles apply:

a) Record maintenance
b) Accountability
c) Sensitivity
d) Evaluation of quality
e) Distribution and best use

7.2 .Report logging

7.2.1 Initial information handling and recording

When an information report (of any kind) is received, it must be immediately logged, preferably twice, once in a hard-copy version, and once electronically. The hard copy provides a backup in case of a computer failure or power outage. A data record tag/slip should be attached

- Unique record number (URN)
- Time (24 hr) and date the report was received
- Time(24 hr) and date the report was recorded
- Method of reporting
- Details of the person making the record of the report (name + contact details)

- Sufficient information to describe the location (where it is stored) and nature of the report
- Report type

URN	Time and date the report was received	Time and date recorded	Reporting method	Contact details of person reporting	Location and nature of the report	Report type

The URN is given to the submitted report by the receiving information unit to create an audit trail of received information. The unit will create a second "open"[23] version of the report if editing or "sanitisation"[24] is required. They should ensure the removal of the source details and allocate a further URN to this report, and cross-reference it to the original. Local (national) policy determines who has specific access to unsanitised reports. The original report must be retained and stored securely to ensure that source information is not revealed.

The source of the information can be either the name or address of the person providing the information or an information source reference (ISR) number e.g. IUU report from IOTC – record "IOTC"

In order to avoid any chance of compromise, the details of the person providing the original information should not be placed in the main body of the report. Items of information from the same source but concerning totally different matters should be recorded on separate IRs. If a single source of information provides several items of intelligence relevant to the same issue that could potentially compromise the source, separate IRs can be considered. This is to avoid a single source being identified who may be the only one to know the sum total of the information submitted.

Location and nature of report means where the report can be found and what format it is in (electronic, hard copy etc)

Type of report includes: IUU vessel list, law enforcement intelligence, military intelligence, VMS position report, observer report, fishing vessel report, other vessel reports, and port inspector's report.

7.2.2 Accountability

Ownership of the information belongs to the originating organisation who assesses the risk attached to it. The person in charge of the originating organisation is the **Data Administrator**, and is responsible for assessing the risk. The receiving organisation is therefore accountable to the 'owners' for maintaining that level of risk and treated as **Sensitive**. Examples of this would include some information from official sources (such as military intelligence) but also observer reports. Observer reports should be treated as material which is '**personally-sensitive'**. There have been incidents where observers have been reported as missing or being injured in suspicious circumstances[25] which makes a strong argument for maintaining absolute confidentiality in the case of reports from this source.

Some material may be especially sensitive and may be restricted in distribution. It should be marked as **Restricted** and distributed in accordance with the instructions of the originating Data Administrator

Open" meaning can be seen anyone

[24] Sanitisation is when details are removed which might identify the original source, if that source is confidential

[25] https://www.msc.org/en-au/media-centre-anz/msc-briefings-statements/fisheries-observers-deaths-at-sea-human-rights-and-responsibilities-of-fisheries-organisations

7.3 Source evaluation

7.3.1 Source grading

The source evaluation is made by the person submitting the information to describe the reliability of the source. This enables the credibility of the information to be established and informs the proportionality of tactical options.

Everyone submitting intelligence has a duty to ensure it is accurate and is corroborated where possible. There are three source gradings:

1. **Reliable** – This grading is used when the source is believed to be both competent and information received is generally reliable. This may include information from human intelligence, technical, scientific and forensic sources. It is important that the two tests of competence and veracity of past information are both met before a source is considered to be reliable. Where either test is not met, **not reliable** should be selected or the ground to doubt the reliability is specified.
2. **Untested** – This relates to a source that has not previously provided information to the person receiving it or has provided information that has not been substantiated. The source may not necessarily be unreliable, but the information provided should be treated with caution. Before acting on this information, corroboration should be considered. This would apply to information when the source cannot be determined.
3. **Not reliable** – This should be used where there are reasonable grounds to doubt the reliability of the source. These should be specified within the IR risk assessment and may include concerns regarding the authenticity, trustworthiness, competence or motive of the source or confidence in the technical equipment. Corroboration should be sought before acting on this information.

7.3.2 Information/intelligence assessment

The report should be graded to describe the reliability of the information.

A: Known directly to the source – Refers to information obtained first-hand, through witnessing it. Care must be taken to differentiate between what a source witnessed themselves and what a source has been told or heard from some other person.

B: Known indirectly to the source but corroborated – Refers to information that the source has not witnessed themselves, but the reliability of the information can be verified through corroboration. This corroboration could come from technical sources, or other intelligence, investigations or enquiries. Care should be taken to ensure that the information that is presented as corroboration is independent and **not** from the same original source.

C: Known indirectly to the source – Applies to information that has been told to but not witnessed by the source: the source does not have first-hand knowledge of the information. However, the source may consider that other source to be “reliable”.

D: Not known – Applies where there is no means of assessing the information. This may include information from an anonymous source (crewman or observer), or outside sources such as fishing vessel reports.

E: Suspected to be false – Regardless of how the source came upon this information, there is a reason to believe the information provided is false. Even if false, it should be recorded so that other information from that source can be treated similarly.

For example, reports from RFMO (IOTC or CCLAMR) IUU vessel lists can be treated as (a) open (b) untested (the source has not been corroborated) unless the information source has been corroborated, in which case it can be rated as reliable. Normally IUU vessel lists can be regarded as ‘good’ intelligence sources but all information from any sources should be evaluated as to the strength of its value.

7.3.3 Information content

The information content should be clear and concise. The information must be of value and understood without the need to refer to other information sources. The body of the report should give no indication of the nature of the source. Where possible, the information should be corroborated and its attribution established.

For ongoing operations (hot pursuit, arrest, or satellite surveillance), the operational reference should be added, noting the operational unit.

7.4 Evaluation and quality assurance of the information report

7.4.1 Report assessment

Once a report has been received by the IUU information unit, it should be further assessed for:

- risks and duty of care issues
- information value
- accuracy and full attribution of the information
- consideration for further evaluation and analysis
- consideration for distribution and requirements for sanitisation.

Any amendment to the report should have an **audit trail**. This may include the resubmission of a sanitised report linked directly to the original report. The unit, institution or person who submitted the report should be contacted if further clarity or corroboration is required on any issue

7.4.2 Sanitisation

Reports should be sanitised for onward transmission by removing material, which explicitly or implicitly identifies a source or sensitive law enforcement methodology.

7.4.3 Intelligence report risk assessment

Before distributing any information, the unit moderator should consider the risks associated with the distribution of information. This consideration should include:

- ethical, personal and operational risks in respect of the source, the intelligence content, its use and distribution;
- consider compliance with any legislative requirement;
- consider the proportionality, accountability and necessity for distributing the information.

7.4.4 Authorisation to distribute

Each organisation should develop a policy to ensure suitable levels of authorisation for the distribution of information. Consideration should be given to distribution outside the ASEAN network.

7.5 Distribution of Information

In order to share this intelligence, there must be:

- a compliance purpose;
- local information handling protocols in place;
- a legitimate need to receive it.

Specific questions need to be asked when considering the distribution of sensitive information or intelligence. For example:

- are there any legal obligations?
- who is asking for it?
- why do they want it?

- what are they going to do with it?

If there are concerns around how widely the intelligence may be distributed, then it may not be appropriate to distribute all of the information and a reduced version may be considered.

The recipient must abide by the handling conditions.

Any intelligence (military or law enforcement) report with conditions should remain under review to ensure that wider distribution can occur as soon as is feasible, such as when an operation has been concluded or is no longer being pursued.

7.6 Audit trail

This is necessary when information or intelligence is distributed. The following information should be recorded:

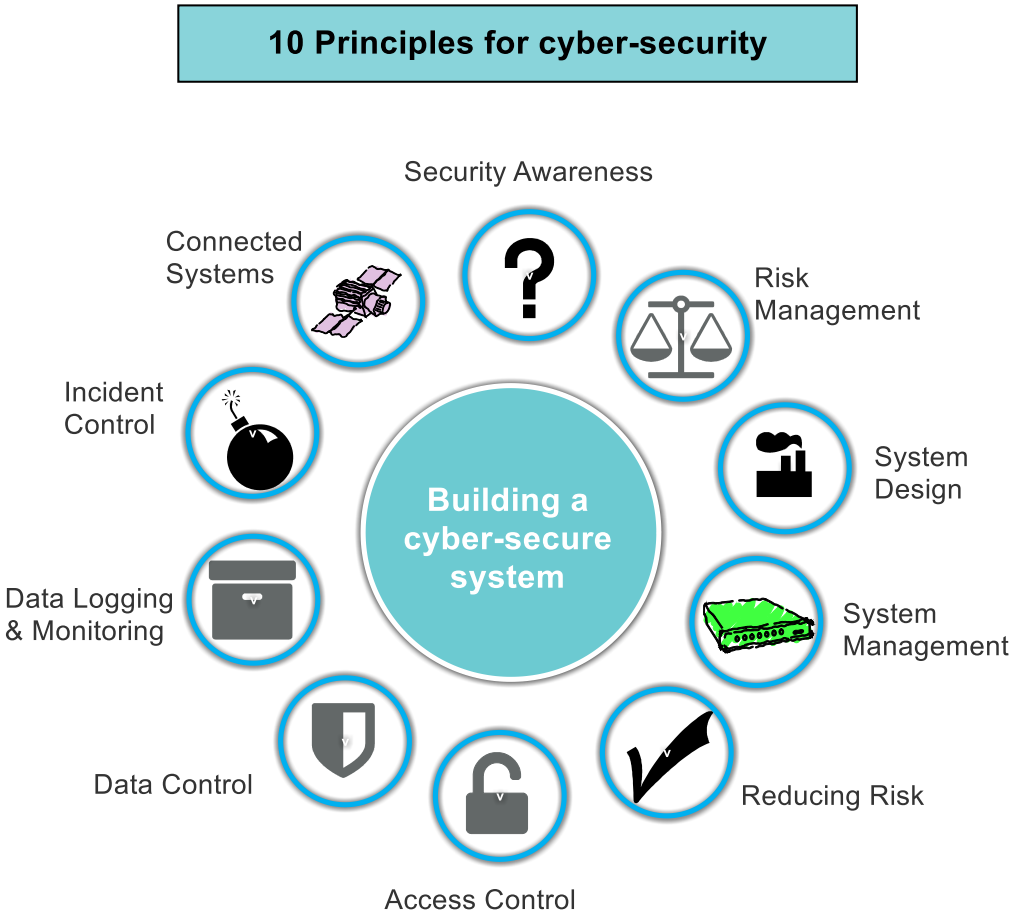
- recipient
- material distributed
- purpose of distribution
- authorisation
- restrictions on the use or further distribution of the information
- additional risk assessment, if appropriate.

The audit trail should enable the ‘trailer’ to follow the trail back to the original source and to check that all necessary steps to ensure the confidentiality of the sensitive material have been taken and that confidentiality has not been compromised.

8 Procedures for cyber-security

8.1 Introduction

Risk is determined by the risk-owner, that is the originator of any information. It is for risk owners to properly understand the value and sensitivity of their information, and how they work with it, in order to make informed, risk management decisions. The purpose of the AN-IUU is to share information and that carries a risk in itself. Sharing anything, but especially information across digital systems opens up the entire system to risk. That risk has to be accepted to gain the benefit of acquiring and sharing information. The risk cannot be removed, since the loss of risk means a loss of information, so the risk must be managed. These procedures suggest how this can be done



8.2 Principles for cyber-security

1. Security awareness and training
   Work with AN – IUU Focal Points to create security awareness and develop on-going training.
2. Risk management
   Identify risk and develop a risk-based approach to managing data and systems.
3. System design
   Build security into the system including management and maintenance.
4. System management

Understand AN - IUU data needs and what the system capacity can support to meet the unit's work demands.

5. Access Control
   Establish controls on who - AN – IUU Focal Points and persons - can access the system. Share this information with the AN-IUU.
6. Data security
   Protect confidential data and identify weaknesses in the system.
7. Reducing risk
   Protect the systems and use continual risk assessment to reduce risk.
8. Data logging and monitoring
   Establish procedures to protect data so that incidents can be prevented and investigated.
9. Incident control
   Anticipate incidents and design the system to respond and recover.
10. Connected systems
    Work with the other units in the network to develop an overall risk control environment.

8.3 Security awareness and training

AN – IUU Center to take responsibility for security environment

- AN – IUU Center should work with all AN – IUU Focal Points to establish a security environment – an attitude of mind and collective awareness of the need for cyber-security. Working collectively will help to instil a sense of shared responsibility. Managers work to uphold the cooperative approach.

Work with staff to be more effective

- Anticipating problems will help to create the security environment and to develop the necessary procedure and protocols to make security functional. A joint approach will help to make the work of the unit more efficient.
- Involve everyone in the process, particularly those with special knowledge, to general security as well as the system's security. Encourage AN – IUU Focal Points to challenge procedures so that the systems are collectively tested and have general confidence. A collective approach means that issues can be identified more quickly and raised for attention early.
- Set in place a reporting system to enable staff to raise issues and have them recorded so that action can be taken and recorded, and, if necessary, re-visited. Reporting should be encouraged and responded to positively.

Promote security awareness

- Promote security awareness.
- Make messages and ideas relevant. Work with AN – IUU Focal Points to create co-operative activities, rather than impose them from above. Ensure that the messages are relevant to AN – IUU Focal Points and tailored to the AN - IUU.
- Develop positive approaches and work to engage AN – IUU Focal Points with the approach, so that ownership is shared.
- The AN – IUU Center should lead awareness but, AN – IUU Focal Points must be kept involved. The AN – IUU Center must be seen to be fully part of the process.
- Awareness is a continuous process and needs to be refreshed from time to time.

Cyber security training

- Develop the training programme to meet AN – IUU specific needs. Pre-set training may not be relevant so consider training needs carefully.
- Keep training discrete and relevant. Better to have short courses than lang training sessions.
- Keep training fresh. Don't re-use material so that it becomes stale. Make sure training encourages responses from AN – IUU Focal Points.
- Bringing in trainers can be valuable but any outside trainer(s) should be made aware of the work undertaken so that training can be tailored to the specific needs of theAN - IUU.

8.4 Risk Management

Consider the risk around the work environment

- Consider the work of AN - IUU: main focus, priorities and external connections. Consider the technology involved and where its weakest points are. Build up a picture of overall risk. The picture you build up will identify the risk and the decisions you need to make to confront cyber risks.
- Develop a policy that meets AN – IUU goals.

Know where risk is most likely and how to manage

- Consider the AN – IUU Interactive Platform system's technology, services, data sources, data storage, internal and external links.
- Create and review an outline diagram of the system. Identify all link and data storage, including the cloud. Work with AN – IUU Focal Points to ensure that the diagram is as complete as possible.
- The diagram should include all links and features that are outside of control, including outside services.

Make sure the risk management strategy fits the work environment and institution

- There are many approaches, so, choose one that makes the best fit.
- Purchase effective anti-virus systems which can be regularly updated
- A careful risk assessment can be used as the basis for an off-the-shelf package. You will need to consider carefully if the risk is likely to be technical or non-technical. If it is non-technical then AN – IUU Center procedures should deal with risk. Technical risks may require outside expertise. An outside expert may need to carry out its own risk assessment, in which case the system diagram will be an essential component of developing that strategy.
- It may be that the strategy may involve a range of different approaches. In any case, it is important to make sure that the approach and the reasons for choosing it should be properly documented.

Recognise the risks and how to manage them

- The strategy, guided by the system diagram, should be used to identify risks and how to manage them. Carefully identify the steps needed to eliminate or reduce risk, and make sure that these are written down. Be clear about what risks you can deal with and what risks will need outside expertise to manage them.
- If the risk is to be managed externally, then ensure that the risk control systems can be put into action quickly, and at any time.
- Ensure that the risk management strategy is one that has the confidence of the AN – IUU Focal Points.

Make sure cyber risks and risk management are understood by AN – IUU Focal Points

- It is the AN – IUU Center responsibility to ensure that all AN – IUU Focal Points understand the risk management strategy. If they understand, it will help to make decisions effective.
- The strategy message must be clear and understandable by everyone. Ensure that the risks are clearly identified and can be quantified in terms of financial or legal risks, as well as administrative risks.
- Clarify risk so that action can be taken effectively. Categorise risk as Severe, Medium and Low. Make sure that each level is well understood.

Risk management is a continuous process.

- Risk is continuous and so is managing it. Upgrade the strategy regularly.
- Review the risks and system diagram regularly.
- Any changes to the system, new equipment or links or services will need to review the system diagram and upgrade the risk management strategy.
- Keep updated on risk and make sure your review is carried out regularly, annually or six-monthly.

8.5 System design

Understand what you are building and why

- Make sure you understand the purpose and demand and outputs before designing a system, including the risk and threats. Make sure that these are understood by the AN - IUU before you proceed. Clarify the threats and design the system around them, not forgetting external links.
- Make security controls, security packages etc as part of the overall design of the system.
- Project the lifetime of the systems and try to identify future demands and risks. Allow the system to evolve with time.

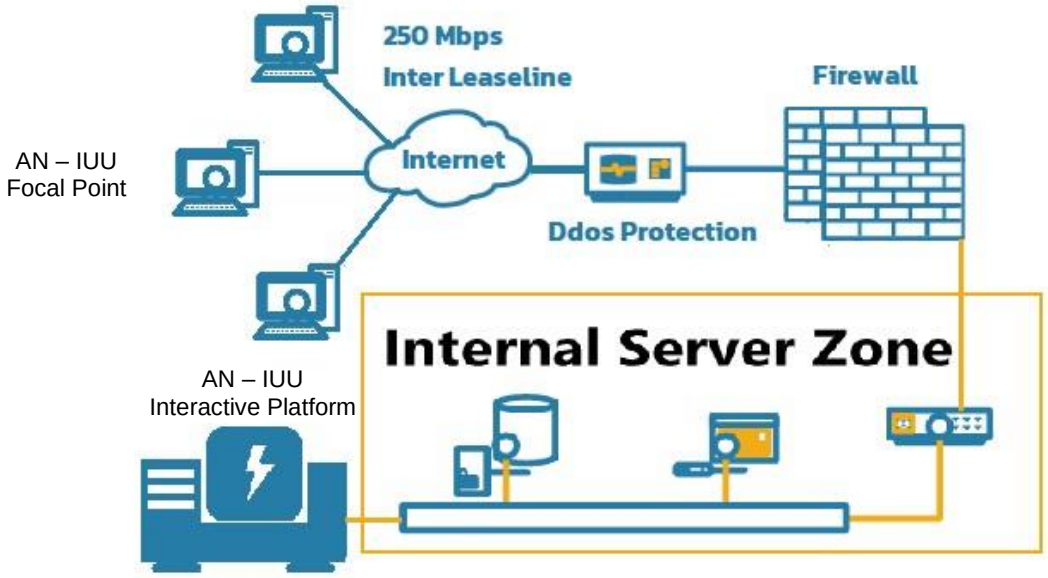


Figure 2: System diagram

Maintenance and updating should be simple

- Consider what can be bought locally, off the shelf. Make sure that servicing and replacements are easy to acquire and KEEP IT SIMPLE. Complications tend to make difficulties. Make sure programs are easy to understand and that training is available. Chose a reliable supplier.
- Consider the cloud and include the use of the cloud with the security risks.
- Build security into the system, rather than as a bolt-on after it has been put in place. This will reduce risk.
- Work with the supplier to ensure that the system can be updated over time.

Build-in security and reduction of supply disruption

- Make the system secure by building layers of security so that any attack has to deal with more than one portal. Allow for immediate shut-down, if necessary.
- Reduce the risk of attack by reducing the number of external entry points. Identify the firewall points. Remove unnecessary links
- Make all servers and external devices secure to reduce risk.
- Do not trust external e-mails and data. Make sure all such items can be validated and subject to firewall checks. Make use of checks so that first-time responses can be validated and trusted before being accepted into the system
- Purchase hardware and programs that have built-in default products and services that are designed to be secure by default. This should be included in any procurement specification.
- Make security procedures easy and repeatable. Complicated systems encourage by-pass habits.
- Make sure you understand the system and be clear about any contractual obligations by the supplier. Ensure that all costs are accounted for and are well understood by both sides.
- Keep to well-tested systems and design. You will be more confident with well-understood systems.
- If the power supplies are erratic, then build in surge protection as well as back-up power.

Maintain a safe security environment

- Maintain the safety of the system and reduce risk. If the system is attacked, the next step is usually to gain access to the data storage and make it inaccessible to you, the owner. The intent is generally to ransom access.
- Maintain updated antivirus programs that can detect threats.
- Develop a backup plan together with a recovery plan. Make sure that this is fully comprehensive for the system. This will enable systems recovery to be made effective.

Make investigation easy

- Make it easy to detect attack risk points.
- Ensure that data is logged and monitored.
- Safely develop and manage systems.
- Use technical and policy controls to ensure that all changes are validated and approved and have been properly checked. Design controls to make it easy to apply security updates.
- Make it difficult to assess the system by using human and machine checks. Change passwords (see Access Identification). Keep your code storage protected with limited access.

- Protect key access points and limit access to the systems administration interface. Confine access to the AN-IUU Interactive Platform administrator and one substitute. Restrict access to administrative interfaces, web consoles, and trusted locations or devices. Use multiple access authentication with separate codes. Keep a written record that can be used in an emergency to access the system, including a 'fail-safe' in case of real failure.

8.6 System Management

Make system management an integral function of your unit management.

- Use the system diagram to review the security in terms of data management, data logging and monitoring. Identify all devices on the system and review the risk in terms of access and weak points for malicious entry. Involve AN – IUU Focal Points in the process and work through problem-solving with them to ensure that the system is well-protected.
- Identify who is the named person responsible for integrating and managing access across the system. The person responsible will cover IT, configuration, device selection management, financial control and service delivery as well as initiating emergency procedures.
- Develop a coordinated approach to managing the system and data as part of your security strategy.
- Make the system 'clean' – simple, removing clutter, unnecessary administration and procedures. Ensure that duplication is removed (apart from essential backups). Make sure that the AN-IUU Interactive Platform administrator can deal easily with issues and ensure that the system is continuously updated. Complex systems create more opportunities for risk

Make sure the systems management can identify linked data and associated devices so that risk can be prioritised

- Make an inventory of all systems assets. This should be updated and, if possible, automated. It is essential that it is easily accessible to help with risk management.
- Keep on top of your technology so that the system remains clearly and easily understood so that critical elements can be identified and protected.
- Have a clear understanding of your data management systems and where data is stored and how it is processed
- The AN-IUU Center responsible for the system management should also be responsible for data management.
- Make sure that there is a data management system that records how data is stored, and how backups are made and where these are stored. The data management system should have its own security protection.
- Work with AN – IUU Focal Points to manage their own digital personality. This includes social media. It is imperative that there is no access by social media to the system. It should be clear at all times that the system being used is for your unit's' official business, and there is no place for private social messaging
- Keep the system diagram updated, together with all portals and internet interfaces.
- Keep the supplier list updated including what assets they are responsible for. This should also form part of the risk management,

Only keep what you really need

- Keep the system focussed on the overall AN-IUU task. Don't add outside interests.

- Only keep data and information that is relevant and is needed. Any accounts that are not relevant or appropriate should be removed or disabled.
- Assets that are no longer useful or relevant should be removed and any information on them should be deleted. This may involve removing hard discs and destroying them

8.7 Reducing risk

Keep the systems updated

- Keep the system automatically updated. You may have to stagger updates if major updates being received have an impact on overall operability. Updating outside normal working hours should be considered. Use this information to develop an updating procedure
- Consider using a contracted service system to maintain updates and general maintenance.
- When procuring software, consider data loading and use of Wi-Fi, make sure that the products are relatively new so that your version stays within date for updating. Consider updated versions as part of the general functioning of the system in case of system over-load when updating.
- Use manual testing methods (for example penetration testing) in addition to automated tools. These methods simulate attacker behaviours to find weaknesses and prove that they can be exploited.

Managing outdated hardware

- If it is not possible to update outdated equipment, make sure that such equipment is isolated from the normal security risk. Consider using a separate access system to continue using the hardware if it is still usable.
- Establish a separate risk management programme to reduce risk to the overall system.
- Generally, maintain updating even if one component is no longer updateable.
- Finally, even if one component of a system is obsolete, always continue to update and patch the other components of the system. For example, continue to update browsers and anti-malware products, even if the underlying operating system no longer receives updates.

8.8 Access control

Establish a unit access policy with clear logging-on systems and identity checks.

- Give consideration to the access policy. Identity control is the first and most important priority. It should be based on:
  - Who has access;
  - Why they need access;
    - What are the reasons for access and,
    - Where they want to access.
- Consider all persons who may need access; AN-IUU Focal Points, ASEC staff, AMS related staff (by country officially request), and associate service providers.
- Make sure that the access policy is backed up by records that can be investigated in case of incidents. No access should be allowed without due identification, address and contacts. All access should be covered by cover references.
- Account services should be capable of restricting access, have time limits for temporary access and immediate blocking of access for a person leaving the unit system permanently.

- If service providers or contractors have access, they should sign access agreements with confidentiality clauses.

Access identification

- Access should be governed by access demands. Not all users will need access to all elements and all devices. The AN-IUU Interactive Platform administrator should establish a multiple-entry-level system, with access to all parts of the systems restricted to as few users as possible.
- Consider using two-factor Data Security authorisation for external online accounts, to maintain password protection.
- The password policy should insist that NO password used by any user should be the same as that person's personal email account.
- Implement technical controls such as multiple layer authorisation, account control, or lockouts, monitoring for suspicious behaviour, and ensure that chosen passwords are string. Use a test subprogram to detect weak passwords.
- Ensure credentials are adequately protected both at rest and in transit.

Monitor use of access to maintain security and reduce risk.

- All access and logging-ons should be recorded on a secure site. Unauthorised or malicious attempts to access the system should be identified and the administrator altered.
- Malicious attempts would include attempts to acquire passwords or multi-level access entries. Likewise attempts from specific areas as well as techniques such as 'password-spaying' and unexpected lock-outs.
- System design should allow for account monitoring. All access from all accounts should be logged and should be traceable.

8.9 Data Control

Protect data to match the assessed risk

- Be aware of the data. It is the most important part of the system and it has value. It needs to be protected from attack and from loss.
- The basic rules for data are:
  - Access to data must be protected
  - Keep important data in one place
  - Don't store unnecessary data
  - Don't keep data on the computer desktop
  - Backup, backup and backup.
  - Keep a system backup
  - Record access events to data, which should be monitored to ensure legitimate use.
  - Protect data that is being transferred.
- Use secure, encrypted and validated access protocols. use application protocols wherever possible and use network layer encryption such as Virtual Private Network (VPN).
- If discs are used then there should be encrypted access controls. External access should be through secure portals.
- Specific access portals should be defined and secured with encryption. Access should be only available to authorised users.

- Ensure that the storage supplier is a well-established entity with a very secure system.
- If there are legal issues about holding data, or who has access to data and for what purpose, then these should be made clear and a legal notice posted with each access attempt.

Data backup

- Maintaining backups is essential. This is the main purpose of the system. Backups must be secured against accidental deletion of destruction. Recovering data whether from accidents or malicious attacks is critical to the work of the AN-IUU Center.
- Offline backup is an important part of the data security plan. This MUST be kept separate from your own network and the cloud, if used. This backup must be kept separate from all users, under the direct control of the AN-IUU Interactive Platform administrator . Protecting this reserve, with a hard disc to protect the data from attack. Access to the unit must be protected.
- Put a time limit on backups. Continuous backup can be liable to virus infection. Make a disc or hard drive version to be stored. The time limit will be one, which is dependent on your own data generation. But a probable turn-around time would be around 6 weeks.
- Give a trial run from time to time to ensure that the recovery procedure works and that you have a good understanding of how to carry this out.

Disinfect the storage media from time to time.

- To reduce the risk of re-infecting files when recovering data from backup storage, ensure that .exe files can be restored from reliable sources rather than from the backup, to reduce the risk of re-infection.
- Create a re-use and repair plan from any data storage or online devices (including peripherals) to ensure the risk of re-infection is reduced. The repair plan should include ‘disinfection’ (sanitisation) procedures to meet risks. Some storage items, such as Solid-State Discs can be difficult to effectively sanitise so these may have to be destroyed from time to time.
- All disposed-of data storage MUST be effectively destroyed e.g. by breaking the glass of hard discs. All labels and other means of identifying the content should be removed.
- The sanitisation plan should cover all new hardware. The plan should ensure that all data is being properly used and that all elements within the system are properly tested and sanitised,

8.10 Data logging and monitoring

Logging and monitoring

- The purpose of logging is to create a record that can be examined in case a malicious attack or other forms of data security breach take place. It is better to maintain the log in your own system.
- The use of the log will enable to answer these questions
  - What happened?
  - What was the impact?
  - What are the next steps?
  - Was our response effective
  - Did our security check work, and if not, why not

- The aim must be to understand what happened during an incident and what to do.
- Know where the logs are stored and what to look for, even if the search is sometime later.

Signs of an attack

- Check if the system has interrogated a suspect IP address. Network Address Translation (NAT) should be used on the network to identify the internal and external IP details.
- Has any device been asked for an external domain name or URL?
- Has any member of AN-IUU Center staffs/ AN – IUU Focal Points received a suspicious email linked to any of the above, including downloads? Check on web proxies.
- Use specialised programs (discuss with the supplier) to investigate if any staff member's hardware has been used. Check if particular links have been clicked on.
- Check host logs for process information, DNS lookup events, file system changes, file hashes, web requests, and any other traffic.
- Check which devices have been used and who was operating that device.
- Keep the logs long enough to be able to be interrogated effectively. This will involve establishing volume, access and availability of storage,
- Decide which logs should be kept in a central site. Consider encryption as a part of this plan. Ensure that the logs are examined to determine if they are capturing the required data.
- Keep the logs protected from any unauthorised access or tampering. Any access should be recorded on logs in another site.

Logs are useful tools

- A good logging system will enable you to check on use and judge the effectiveness of the system.
- The log facilitates monitoring of use and what sites are being accessed. Knowing that sites that are accessed are also recorded informs staff as to safe and responsible usage of the system

8.11 Dealing with security incidents

Make a security event response plan

- Test the system with mock exercises and update the plan with what you learn from both real and mock security events.
- The plan must be closely aligned with the logging and monitoring strategy.

Incident control.

- A good plan will help to detect and control incidents. Learning from mistakes is expensive but not as expensive as NOT learning from mistakes.
- Involve the right people in the plan. This will include not only the AN-IUU Interactive Platform administrator but may also include the suppliers and service providers. Your institutional management must support your plan. Consider what other organisations may need to be contacted in case of a cyber-attack, especially if this has national security implications.
- Include how alerts will be actioned and who must respond to them.
- Each person involved in the plan should have an assigned role and set of tasks. Make sure that each person has a written document, combined with other documents to be used in the case of an absolute failure when the computers may not be accessible. A contact list should be included with all contact details, including other useful contacts,

- The security event plan MUST be linked to recovery. This is its prime task.
- Work with the supplier to identify HOW incidents will be detected. Consider how you will detect incidents and what the methodology will be.
- Decide how you should deal with serious threats and increasing problems. At some point, National Security may need to become involved.
- Make the AN IUU Center staffs aware of the plan and what their roles may be. Also, what they should do to alert in case of an attack.
- Create a list of authorities and who should be contacted and who can authorise each next step. Technical staff will need to be aware of this.
- Be aware that at times, technical staff may not have time to seek authorisation. Plan for this. Delay can make matters worse. Allow for a fast-moving situation.
- Ensure the plan includes basic guidance on legal or regulatory reporting requirements based on the types and volumes of data your organisation holds, and an outline of the processes covering a full incident lifecycle. An example plan is shown below.

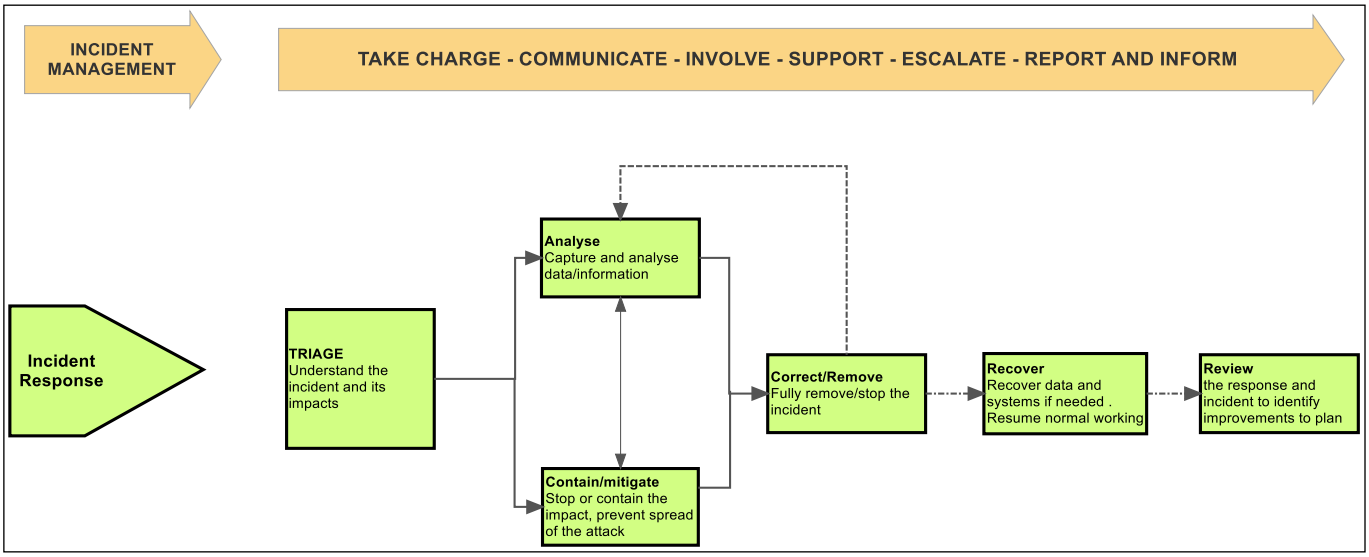


Figure 3: Incident control

Practise the plan and practice communication

- The plan will need to be gamed.
- Make sure all AN-IUU Center staff know their parts and communicate what has to be done. Keep it simple but effective.

During the security event

- As the AN – IUU Interactive Platform Administrator, keep calm. If there're is a financial threat – ransomware – immediately communicate with AN – IUU Center and with the responsible national security agency.
- Keep AN-IUU Center staff informed and communicate clearly with them. You should have built up a level of trust; use this to ensure good working.
- Assign one AN-IUU Center staff to keep a written log of events.
- Use the log to substantiate your actions.
- Remember doing what is rights is usually the right thing to do.

After the security event

- Update all plans, Gather staff to discuss what happened. Keep records of the meeting so that all comments can be recorded. Learn from mistakes.
- Review all logs carefully. Identify any weaknesses and protect these.
- Be truthful. Don't attempt to escape mistakes but also identify what worked as well as what didn't. The new plan must be better than the last.

8.12 Connected systems

- When you make the system plan, ensure that all external links including other members networks are included.
- Make sure ALL external links are included, (other networks, suppliers and service providers). Repetition of the previous point?
- Work with service providers to make sure the system is well understood. Make use of their knowledge to improve the system.
- Learn what their security system is and see if it can be used to improve the AN-IUU Interactive Platform security system.

Procurement and contracting

- Make sure that these processes are included in the security plan, especially with courtside contractors, including sub-contractors.
- Look for information published by your existing commodity suppliers that help you understand package information and what it offers. Remember that this is part of the contract.
- Your suppliers have their own security procedures, make sure that these meet your standards.
- Work with your supplier to develop a common interest in the success of the system being installed.

Security MUST be part of the procurement contract.

- Build security considerations into the procurement and contracting decisions, and make your suppliers aware of this
- If using the Cloud, make sure that you understand the security and that the suppliers have a legal responsibility as vendors that the security is effective,
- When making decisions about commodity suppliers like cloud service providers, seek Cloud security guidance for more information on how to determine how confident you can be that a cloud service is secure enough to handle the data.
- Don't use administrative procedures or departmental practices to create problems for your suppliers when designing security.
- Two books have been recommended above but there is another material. Build up your own security library in hard copy. Remember if the system is down then you can't look it up online.
- Make sure that all suppliers and products are checked and are well understood,
- Consider what support you will need from suppliers to maintain their products and services, likewise use vendor or community-supported software where available.

Help the other networks in ASEAN

- If you have had a bad cyber-attack, you will need to inform the other networks for their protection. After the event, share your experience with them and what you did to rectify the situation.
- Learn from their incidents and experience to improve AN-IUU own plans.
- Share with other bodies what your experiences are but also consider who AN-IUU contact.

9 References

Agarwal A, 'Critical Analysis of Doctrine of Hot Pursuit in Respect of Maritime Piracy' (2020) 2 International Journal Of Legal Science And Innovation 685

Allen CH, 'Doctrine of Hot Pursuit: A Functional Interpretation Adaptable to Emerging Maritime Law Enforcement Technologies and Practices' (1989) 20 Ocean Development and International Law 309

Bergh P-E, 'Ex-Togolese Fishing Vessel Changes Flag in the High Seas' (*Stop illegal fishing*, 2011) <https://stopillegalfishing.com/news-articles/ex-togolese-fishing-vessel-changes-flag-in-the-high-seas-4/> accessed 20 August 2020

Boerder K, Miller NA and Worm B, 'Global Hot Spots of Transshipment of Fish Catch at Sea' (2018) 4 Science Advances 1

Chuaysi B and Kiattisin S, 'Fishing Vessels Behavior Identification for Combating IUU Fishing: Enable Traceability at Sea' (2020) 115 Wireless Personal Communications 2971

Chuvakin, Anton A., Kevin J. Schmidt. Logging and Log Management: The Authoritative Guide to Understanding the Concepts Surrounding Logging and Log Management, 2012

FAO, *International Plan of Action to Prevent, Deter and Eliminate Illegal, Unreported and Unregulated Fishing.* (FAO 2001)

Forum Fisheries Agency; and Tracking TM, *Photo Manual for Fisheries Air Patrols: The Use of Cameras to Support Fisheries Aerial Surveillance* (Forum Fisheries Agency 2020)

Freestone, David. & Food and Agriculture Organization of the United Nations. 1998, *The burden of proof in natural resources legislation : some critical issues for fisheries law FAO Legislative Paper No. 63/ by David Freestone* FAO Rome

Gibson T, 'The One That Didn't Get Away' [2001] Journal of the Australian Naval Institute 22

Gomez G and others, 'The IUU Nature of FADs: Implications for Tuna Management and Markets' (2020) 48 Coastal Management 534 <https://doi.org/10.1080/08920753.2020.1845585>

Hsu FC and others, 'Cross-Matching VIIRS Boat Detections with Vessel Monitoring System Tracks in Indonesia' (2019) 11 Remote Sensing 1

Interpol, *International Law Enforcement Cooperation in the Fisheries Sector* (Interpol 2018)

Kernighan, Brian W.. Understanding the Digital World: What You Need to Know about Computers, the Internet, Privacy, and Security, Second Edition. Princeton University Press.

Law Commission, 'The Admissibility of Expert Evidence in Criminal Proceedings in England and Wales: Recapitulation and Review' (2009)

Liddick D, 'The Dimensions of a Transnational Crime Problem: The Case of IUU Fishing' (2014) 17 Trends in Organized Crime 290

Miller DD and Sumaila UR, 'Flag Use Behavior and IUU Activity within the International Fishing Fleet: Refining Definitions and Identifying Areas of Concern' (2014) 44 Marine Policy 204

Molenaar EJ, 'Multilateral Hot Pursuit and Illegal Fishing in the Southern Ocean: The Pursuits of the Viarsa 1 and the South Tomi' (2004) 19 International Journal of Marine and Coastal Law 19

MRAG Asia Pacific, 'Towards the Quantification of Illegal, Unreported and Unregulated (IUU) Fishing in the Pacific Islands Region' 1 <http://www.ffa.int/files/FFA Quantifying IUU Report - Final.pdf>

Nagosky DP, 'The Admissibility of Digital Photographs in Criminal Cases' (2005) 74 FBI L Enforcement Bull 1

North Atlantic Fisheries Intelligence Group and INTERPOL., 'Chasing Red Herrings: Flags of Convenience and the Impact on Fisheries Crime Law Enforcement' (2017) <https://fishcrime.com/wp-content/uploads/2017/09/Chasing-Red-Herrings-Report-Email.pdf>

Russo T and others, ‘Assessing the Fishing Footprint Using Data Integrated from Different Tracking Devices: Issues and Opportunities’ (2016) 69 Ecological Indicators 818 <http://dx.doi.org/10.1016/j.ecolind.2016.04.043>

Stop Illegal Fishing, *Evidence Collection Manual For Fisheries Enforcement: Implementing Port State Measures* (Stop Illegal Fishing 2020)

Trygg Mat Tracking; and Stop Illegal Fishing, *Photo Manual for Fisheries Enforcement* (FISH-i Africa)

Walker R, ‘International Law of the Sea : Applying the Doctrine of Hot Pursuit in the 21st Century’ (2011) 9 Auckland University Law Review 194

Wold C and Cook A “Bubba”, ‘Shining a Light on High Seas Transhipment: The Need to Strengthen Observer Reporting of Transhipments in the Western and Central Pacific Fisheries Commission’ (2020) 26 Hastings Environmental Law Journal 185

.

Annexes

1. Verifying Illegal, Unreported and Unregulated Fishing Vessel

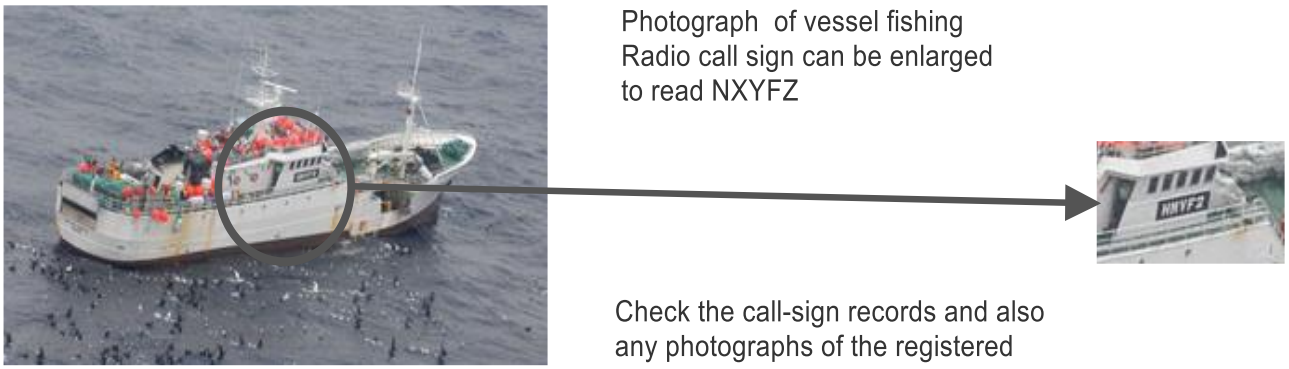
Identifying a vessel or associated vessel, as being involved in IUU fishing is a serious allegation and any such report must be verified so that the allegation can be substantiated. The following steps[26] are advised and while those steps are being undertaken, the person carrying out the work is advised to make a record of the checks made and to file a copy (written or electronic) with the original report. This is so that any later objection to the identification can be responded to by showing that all necessary checks were made.

1.1 Checks to Illegal Fishing

When a report is received that a national or foreign vessel has been detected fishing, or carrying out "fishing-related activities" (see definitions) in a State's waters (internal, territorial or EEZ) and it is *alleged* that the vessel is not authorised to do so, then the following checks should be carried out before any further action is taken:

Step 1 Confirm vessel name, call sign (IRCS) and registration number

Check the national vessel licence record - permits or authorisation register - to establish whether or not a fishing permit has been issued by the coastal state authorising the vessels to fish in its waters



Check authorised fishing zone given in the permit. Is the vessel authorised to fish in the zone where it was sighted?

If the vessel is fishing in the EEZ, then the relevant coastal state should have information on all vessels authorised to fish in their EEZ, listed in their national fisheries system.

Step 2 No national authorisation is issued to the vessel

If there is no record of a permit to fish issued to the vessel to fish in (for example, the coastal state's EEZ) then contact the AN-IUU to **check authorisations** to fish under any sub-regional arrangements to which the coastal state may be a member.

Step 3 No record of regional (or sub-) authorisation

[26] FFA. Best practice guidelines for a data analysis unit.

If the vessel is not recorded as being authorised to fish under any regional or sub-regional arrangements, then, **check the relevant RFMO's Record of Fishing Vessels**[27] database to determine whether the vessel is registered on the approved vessel list to operate within the Convention area.

Also **check the SEAFDEC Regional Fishing Vessels Record (RFVR)** to see if the vessel is listed on it.

Step 4 No record of vessel on RFMO Record of Fishing Vessels

If the vessel is not registered on an RFMO Record of Fishing Vessels (RFV), then **check other open vessel registries for additional vessel information**.

a) **Check other RFMO records of fishing vessels**, members states, Vessels of Interest (VOI), combined IUU listings (e.g. https://iuu-vessels.org/) and other information to determine:
   i. whether or not the vessel is permitted to fish/operate in that organisation's area,
   ii. Determine what is the flag state of the vessel.
b) **Check with the coastal state administration** to establish whether the presence of the suspect vessel, detected in its waters is known or permitted.
c) **Check registries** and ensure that the International Radio Call signs (IRCS)/Marine Mobile Station Identification number (MMSI)/ Unique Vessel Identification (UVI) number[28] and name and other vessel particulars are distinct and can be linked to the suspect vessel. The IMO number may be available but many IUU vessels do not have IMO numbers.
d) **Check National/Regional VMS and AIS** data/information and track records to confirm alleged illegal fishing activities.
e) **Check previous sightings and boarding reports** to determine if the vessel has been previously seen or boarded. Check other agencies' (military, coastguard/fisheries/police) boarding and at/port Inspection reports, including aerial and maritime surveillance reports.
f) Confirm vessel's flag (of registry) and vessel owner's details from available information sources and communicate through the AN-IUU to report the alleged violation.
g) Step 4 No record of vessel on RFMO Record of Fishing Vessels

Step 5 Make a final check through**.**

Carry out a final determination including rechecking IUU lists, including the RPOA list, and record the flag state response to the sighting report and the allegation of illegal fishing.

If the vessel is registered and data kept within a regional record of infringements; carry out an examination of past records or/and intelligence reports on the vessel to establish a track record of illegal behaviour.

Step 6 Check Catch Documentation Schemes

Check port records and catch records (CDS) to verify catch data against origin, weight, species composition and check whether or not catches were made in accordance with national rules of the relevant RFMO Control and Conservation Measures (CCMs).

Step 7 Present verification process

[27] Or Record of Authorised Vessels (IOTC)
[28] *Unique Vessel identifier* from the FAO Global Record of Fishing Vessels, Refrigerated Transport Vessels and Supply Vessels. https://www.fao.org/global-record/background/unique-vessel-identifier/en/

Recheck that all the steps in the verification procedure have been carried out properly, and that all sources have been itemised. Present the paper showing the process carried out to the officer in charge for further action.

1.2 Analysis to determine Unreported Fishing.

Differences between reported, but unobserved, catches and catches validated by observers' reports have shown that estimates of Unreported catch and effort data can be detected from fishing vessels' catch log sheets through analysis.[29] MCS operations can be used to board and check data and sample catches to deter unreported fishing. But Such programmes are not fully implemented across the region and it should be recognised that patrolling and boarding is costly.

Unreported catch estimates, setting positions, species composition and other necessary information are required by fisheries scientists for resources management. Fisheries statistics cross-checked and verified by analysts are part of national and regional monitoring activities. To these national and regional programmes and activities can be added; transhipment monitoring, port sampling activities, observer reports, particularly comparing these to the vessel reports, catch documentation schemes and electronic reporting and monitoring.

Method for estimating unreported or misreported catches

- *Observer reports:* It is difficult to assign an accurate estimate of the difference between observer reports and vessel logbook reports. This is often dependent on the experience of the observer and the type of fishery being observed. A rule of thumb could put the accuracy of this at around 20% but this is very variable.[30]
- *Trade reports*: Comparisons of trade information from different sources to verify information provided by vessels.
- *Port sampling*: Sampling at unloading ports and in markets, to determine the quantities, species and likely origin of products. Analysing these estimates against reported quantities, species and origin of products from catch documentation systems;
- *Analysis of 'real data' with reported data*: Comparing catch and effort data from observer reports, vessel logs and against electronic monitoring data in order to estimate likely catch, including bycatch.
- *Logbook analysis*: Analysis of long-term logbook data can be a useful means to identifying misreporting, if not deliberate misinformation of the amount not reported. Continued deliberate misreporting tends to develop into a pattern of repetition which can be identified. Comparisons of verified catch (for the same type of fishery and area) can then be made to make an estimate of the 'real' catch.

1.3 Verifying Unregulated Fishing.

Flag states are responsible for regulating the actions of vessels flying their flags on the high seas, under the 1993 FAO Compliance Agreement.[31] Coastal states only have compliance authority over non-flag vessels if they are parties to a regional fisheries management organisation, and then may co-operate to enforce the CCMs of that RFMO.

[29] Chris Wold and Alfred "Bubba" Cook, 'Shining a Light on High Seas Transhipment: The Need to Strengthen Observer Reporting of Transhipments in the Western and Central Pacific Fisheries Commission' (2020) 26 Hastings Environmental Law Journal 185.
[30] MRAG Asia Pacific, 'Towards the Quantification of Illegal, Unreported and Unregulated (IUU) Fishing in the Pacific Islands Region' 1 <http://www.ffa.int/files/FFA Quantifying IUU Report - Final.pdf>.
[31] [FAO] Agreement to Promote Compliance with International Conservation and Management Measures by Fishing Vessels on the High Seas, 24 Nov., 1993, 33 I.L.M. 968 (1994)

Unregulated fishing on the high seas[32] is where a vessel that is

(a) Within an established RFMO area and
    i. Is (apparently) without nationality i.e. not flying a flag or has a discernible port of registry displayed on the hull or on the superstructure; or
    ii. Flying a flag of a state not a party to that RFMO; or
(b) A ”fishing vessel (or ”entity”)” which is fishing not in accordance with the RFMO CCMs, or directly contrary to those CCMs.
(c) Fishing by a vessel in an area where there are no CCMs or other conservation regulations but where the fishing is carried out so as to contravene the duty of the State, under International law, to ensure that its vessels fish in accordance with international agreements.[33] This is a flag state issue.

There may be issues with unregulated fishing within the national waters of member states. This will be dealt with by the states involved. Product from such sources entering the legitimate supply chain can compromise the access of seafood products to the export market.

A considerable amount of unregulated fishing occurs on the high seas and – particularly – on waters adjacent to the EEZ of coastal states. What are known as “Areas Beyond National Jurisdiction” (ABNJ) while outside any state’s control, they may be within the area of an RFMO and likewise coastal states, as flag states, have jurisdiction over their vessels operating in the ABNJ.

Steps to be followed and data sources to be used for unregulated fishing are the same as for illegal fishing.

Step 1 Identify vessel

Identify and search vessel details on national, regional and global vessel registers.

Search vessel on various IUU listings for history of non-compliance.

Step 2 Contact flag state

Liaise with flag state and vessel owners if flag state and ownership is known/established

Step 3 List the vessel as IUU

Follow the listing procedure for the relevant listing body (AN-IUU, RPOA or RFMO (on the relevant website) to list the vessel as an IUU vessel on the RFMO’s IUU Vessel List. Only do this if the flag state and ownership is not known, ***or*** no action has been taken or is intended by the flag state. You should give the flag state due notice (5 days) before taking action and advise them that that is the action you intend.

Step 4 Action if the vessel comes within national jurisdiction

If the **vessel comes within the national jurisdiction** of a member state, contact the appropriate authority in that state and provide the relevant information (VMS, sighting data, photographs) to provide the appropriate agency with the necessary information to board and inspect the vessel with a view to possible arrest.

Step 5 Action if the vessel is not within national jurisdiction

If the vessel is outside the national jurisdiction of any member state, then **continue to monitor VMS tracks** on (VMS/AIS etc) if possible. If the vessel nears a member state’s waters, then inform the states with the position and other information and liaise with the appropriate agency, in the event that a boarding and inspection team is mobilised for action once the vessel comes within the member’s states’ jurisdiction.

[32] Paragraph 3.3.1 of the IPOA-IUU.
[33] Paragraph 3.3.2 of the IPOA-IUU

Step 6 Further action

Contact the legal adviser to take appropriate legal action for an infringement of the RFMOs CMMs.

2 Use of photographic information

2.1 Introduction

Photographs can be valuable when used as evidence, either by providing clear identification of a ship and its activities or by helping the court to understand the scene. Using photographs means talking care that there is a clear understanding of the circumstances in which the photograph(s) was (were) taken and that there can be no accusation that such evidence has been faked. This section therefore will discuss the use of photographic information. The main emphasis will be on the use of such material as evidence but there will also include a discussion on directed photography and the identification of fishing vessels.

This section will not deal with the technical issues associated with photography or over-flying patterns for identifying and photographing fishing vessels; there are comprehensive manuals available which can provide this information and interested readers are advised to consult these. (See: Forum Fisheries Agency[34]; FISH-I Africa;[35] Stop Illegal Fishing[36])

A set of silhouettes and photographs of the main types of fishing and support vessel is given below:

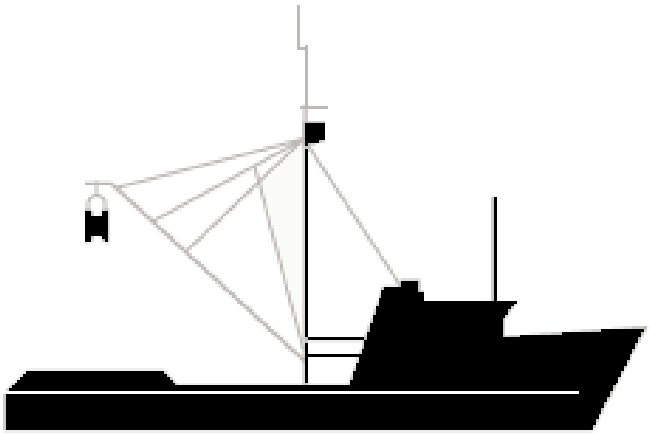


Figure 4:Purse seiner

[34] Forum Fisheries Agency; and Trygg Mat Tracking, *Photo Manual for Fisheries Air Patrols: The Use of Cameras to Support Fisheries Aerial Surveillance* (Forum Fisheries Agency 2020).
[35] Trygg Mat Tracking; and Stop Illegal Fishing, *Photo Manual for Fisheries Enforcement* (FISH-i Africa).
[36] Stop Illegal Fishing, *Evidence Collection Manual For Fisheries Enforcement: Implementing Port State Measures* (Stop Illegal Fishing 2020).

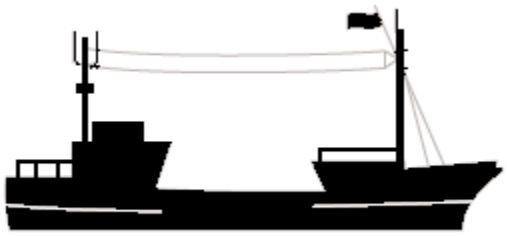


Figure 5: Pole & line vessel

Figure 6: longline vessel

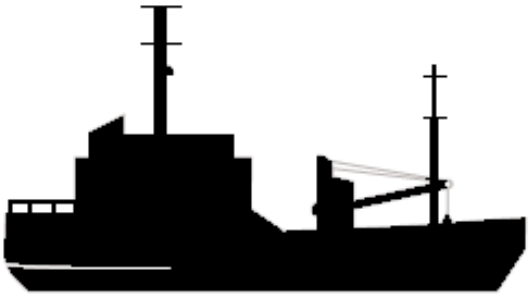


Figure 7: Reefer/ Carrier vessel

Figure 8:(Stern) trawler

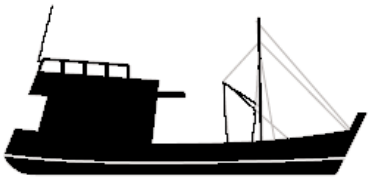


Figure 9:"Blue-boar"

2.2 Aerial photography

A dedicated fisheries patrol aircraft will have (recommended) an automatic camera, linked to the aircraft positioning system (GPS). This means that photographs taken by the camera will have the position, data and time “stamped” on the photograph when the shot is taken. Pre-flight checks as to the accuracy of the equipment are essential.

Generally, this type of equipment is expensive, especially if infra-red and tracking equipment is included for night flights, linked to the aircraft instruments (Instrument Flight Rating). Because of the cost, it will be more usual for hand-held cameras to be used by observers on board the aircraft. In these cases, it is best to have two observers (inspectors on board) with one person taking the photographs and the other recording the position (given by the aircraft commander, or by the 2nd observer, sitting in the front, next to the pilot. This record, together with the photograph number, should be sufficient to satisfy a court of its accuracy

Although the choice of aircraft is a special subject not suitable for these procedures, one point which should be made is that the aircraft should be able to operate at relatively low speeds. Greater accuracy can be achieved at slower speeds, and accuracy is the key output for success in prosecution.

The photographs on the right are aerial photographs of fishing vessels transhipping fish at sea to carrier vessels.

Source: Illegal, Unreported and Unregulated (IUU) Fishing: A Whitepaper. Packard Foundation, 2015

This type of photographs is a very common type of activity that will be photographed from the air

Source: Global Fishing Watch

2.3 Photography for evidence

Photographs and videotapes can also be extremely valuable as evidence because they record details that may have escaped the attention of the observer at the time but which may prove vital at a later stage, particularly to disprove any incorrect statements made by the defence. Wherever possible the cameras should be set to record the date and time on the picture or video-tape. The photographer must keep the film in a secure place after it is removed from the camera and must record exactly what is done with it (e.g., how the photographs were processed and by whom) so that he or she is in a position to confirm in court that it was not tampered with. (In some countries this evidence may be given by way of an affidavit).

Hasty activity on the deck, dumping of gear or fish, fresh fish offal in the sea, sea birds feeding, ropes or gear over the side are all indicators of fishing. Photographs and videos with time and position notations are particularly useful to record this evidence. If the vessel is acting appropriately or after the trial, the photographs can be used for training purposes. The more observant the fisheries officer and the more accurate the notes, the easier it will be to reconstruct the events to decide whether to lay charges, which charges should be preferred, and how to prosecute the case

Photographs are a rapid method of indicating the state of the vessel and gear on arrival on the vessel.

2.4 Photography for vessel identification

Photographing vessel for identification purposes is an essential part of the inspector's work, as is identifying a vessel from photographs taken during patrols. The main identifications of a ship are:

Identifier	***Where usually found***
Name	(1) on the stern and (2) on the side near the bow

Port of registry	(1) On the stern underneath the vessel name or (2) stern trawlers and purse-seiners (that use the stern for fishing operations), on the side, usually near the stern.
Registration (national) number	On the side of the hull, sometimes forward near the bows, or sometimes, on the side of the bridge.
IRCS	Should be on the side of the bridge but may be written on the side of the hull
IMO №	(Unique identifier for ships of 100 GT+) On Hull or bride.

The silhouettes below indicate the most probable locations for each identifier but note (see photographs) that actual practice can mean that identifier location can vary

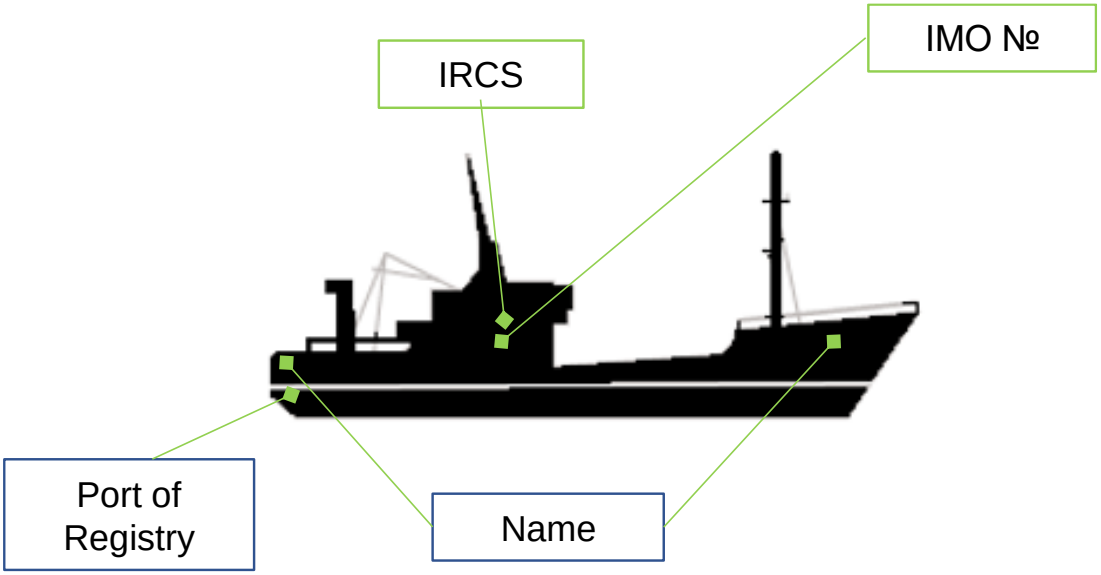
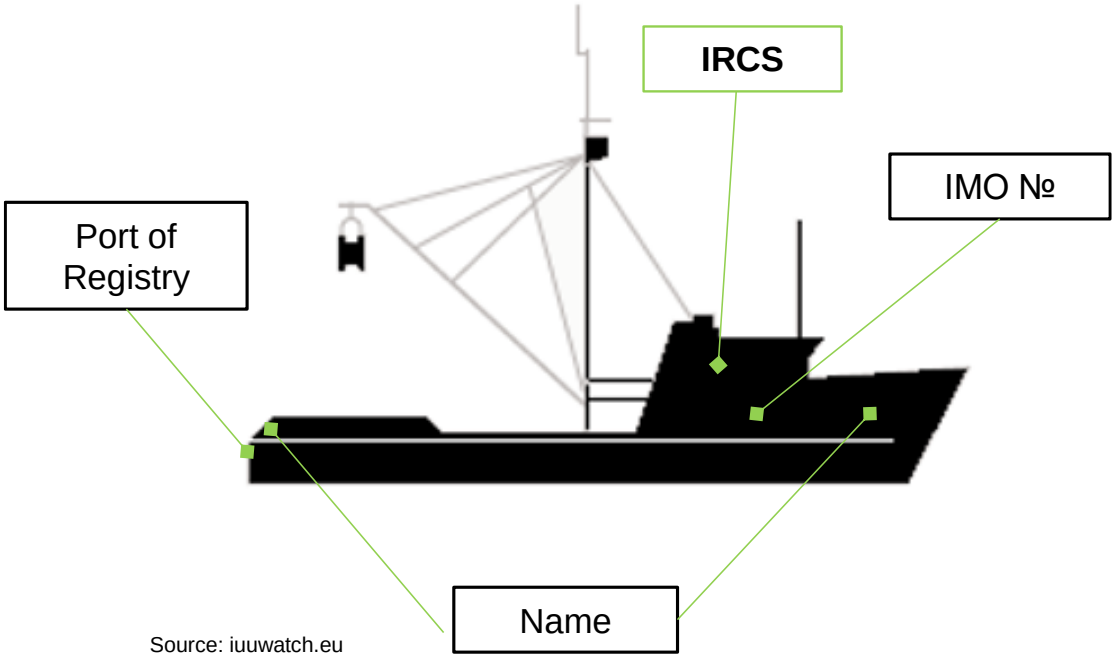


Figure 10:Longliner silhouette showing identifier locations

Note That the ship's name is on the stern but the port of registration is not given in roman letters. Also note the Chinese characters which can be used as identifiers, if the vessel changes its name (in roman characters) but these name changes, carried out overseas, can often result in the original Chines characters being unchanged.

This longliner (note the characteristic slot cut into the side to allow retrieving the catch). This vessel is showing its registration number but there is no discernible IRCS shown.

Figure 11: Purse-seiner silhouette showing identifier locations



Source: iuuwatch.eu

Source: iuuwatch.eu

Note IMO number on stern of carrier

Note purse-seiner name on back of skiff

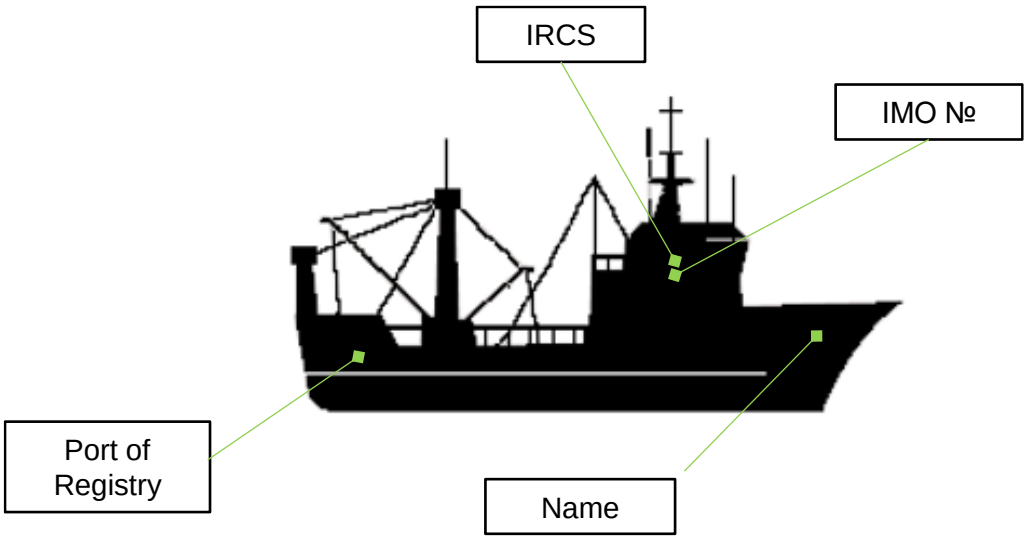


Figure 12: Stern trawler silhouette showing identifier locations

2.5 Presentation of photographic evidence

Previously pictures were made with a camera using photographic film but now the most usual means is to use digital images made using either a camera or a mobile phone. In either case, the basic principle which underlies the validity of presenting photographic evidence to a court is that the court must have confidence that (a) the photograph is a truthful witness to the event or the object(s) being photographed and (b) that the photograph can be exactly located in place and time.

To achieve the first of these two objectives requires that the original image is capable of being verified. This is because the original is recorded data and any image produced is a copy of that original. For this to be admissible as evidence, this copy must be capable of being "authenticated".[37] Consequently, it is necessary to protect the original digital record and then to follow a procedure that maintains that verifiable authenticity, this will involve:

- "chain of custody",
- image security,
- image enhancement, and
- release and availability of digital images.[38]

Based on the above, when presenting photographs as evidence, the points which need to be understood and kept in mind are:

- A photograph purports to be direct evidence of an activity or identity specific vessel. Therefore, it must be shown to an accurate record;

[37] UK House of lords. Select Committee on Science and Technology *Fifth Report*
[38] David P Nagosky, 'The Admissibility of Digital Photographs in Criminal Cases' (2005) 74 FBI L Enforcement Bull 1.

- TWO sets of photographs should be made, one of which should be recorded and stored as evidence. If the picture is to be used in a prosecution, then the memory card should be taken out of the camera and stored with the photograph. This is so that the sequence - and dating – of the photographs can be checked independently.
- Cameras, preferably digital, whether fixed in an aircraft or hand=held on an aircraft or ship, should always be checked to ensure that the date and time are properly set, and (where there is a linked GPS), that the location data is accurate. This should be witnessed, and a record made and signed by the witness.
- it is important that the place, data and time are either
    - recorded on the photograph itself with a linked-in camera on board patrol aircraft
    - recorded separately by the photographer in which case the number of the photograph should be also recorded;
- It is useful to make a statement as to what the inspector saw, with the photograph numbers inserted to illustrate the evidence given in the statement.
- In cases a hand-held camera is used, it can be useful to have evidence of the weather at the time – by a contemporaneous photograph - in case the defence dispute the time and date of photographs.
- To protect the original unmanipulated record, it must be safeguarded either by keeping the memory card or storing it on a compact disc which must be readable but not re-writeable. In this form, the data cannot be written over but only copied. The disc (or memory card) should be labelled with the date, time, and place where the photograph was made (geographic/horizontal position), the person making the image and any other relevant data (ship/plane name/number).[39]

A sketch may be acceptable evidence to a court and again the place, date and time should be recorded on the sketch.

2.6 Clarifying photographic evidence

Evidence of identification should always, if possible, be made in context. The court should have no doubt that a photograph of identity is positive proof. A name or number should be clear to read – see below

[39] ibid.

The picture of the carrier (reefer) above does not show the IMO number clearly, This picture on the left is an enlargement, making the IMO number (IMO 85008840) easily readable. On a technical note, the need to be able to enlarge pictures so as to see detail more clearly means that any picture should have a high ISO number (with a large number of pixels). For evidential use, both the original picture, with the indistinct number but showing the complete stern, needs to be presented together with the enlargement so that the court can easily see the source of the enlargement and that the IMO is definitely for that specific ship.

2.7 Photographs as direct and supporting evidence

Some photographs act as direct evidence of an activity taking place. For example, photographs of actual illegal fishing taking place can be given either as direct evidence (with a position and date/time stamp on the photographs from a linked camera) or as supporting evidence to an officer's written statement or as evidence given in court.

Supporting evidence of purse-seine fishing

The picture on the right is of a Patagonian toothfish, caught in a gill-net, and being hauled up onto the fish-deck. The catch was made in a marine conservation area in the Southern Ocean.[40] This photograph, with a stamp giving position and data and time, could be given as direct evidence. An officer's report, stating the position and date/time noted, could be supported by this photograph, presented in its original form..

Source: Pew charitable trusts

The photographs on the right, of shark carcasses, with fins removed, could be put forward as supporting evidence for fish products found, for example, in an operation such as boarding a vessel believed to be fishing illegally.

Source: sharksonline.org

Source:sibonline.com.sb

The photograph, on the left, of trepang (beche-de-mer), could be used as to support a report of an operation. The photograph could be used to illustrate what was found during the operation.

[40] Economist, 22nd January, 2015

Source: This fish

Photographs of shipping labels can be used as direct evidence if supported by the shipping documents themselves. Such photographs could be given in cases where illegal fish products are being 'laundered' through a port.

Source FFA

Care should be taken in deciding what photographs to use and what weight can be put on the photographs as evidence. For example, the use of a large number of fenders along the side of a fishing vessel or carrier is indicative of being involved in transhipping at sea. But this is only indicative, it is not actual proof. Combined with other evidence, such as VMS/AIS tracking, then aerial photographs of one of these vessels, with fenders, could be presented as circumstantial evidence of transhipping at sea.

Source: The National Interest

(For further reading see: Trygg Mat; Tracking and Stop Illegal Fishing: for technical information see: Forum Fisheries Agency; and Tracking TM, *Photo Manual for Fisheries Air Patrols: The Use of Cameras to Support Fisheries Aerial Surveillance* (Forum Fisheries Agency 2020)

2.8 Attestation and labelling of evidence

A useful guide to what should be recorded to attest to accuracy can be seen in the Belize Fisheries Resources Act, 2020, Art. 60 (2) which requires that an officer attests to the evidence he/she is putting forward by recording the details given below:

(a) his name, address, official position;

(b) the name and, if known, call sign of the fishing vessel concerned;

(c) the date and time or period of time the vessel was in the place or area;

(d) the place or area in which it is alleged the vessel was located;

(e) the position fixing instruments used to fix the place or area stated in *(d)* and their accuracy within specified limits; and

(f) a declaration that the Fisheries Officer checked the position fixing instruments a reasonable time before and after they were used to fix the position and they appeared to be working correctly.

In the same legislation, Art 62 (1), there is a requirement for photographs to be presented together with the position and date and time, as below

Photographic evidence.

62.–(1) Where a photograph is taken of any fishing or related activity and simultaneously the date and time on which and position from which the photograph is taken are superimposed upon the photograph then it shall be presumed unless the contrary is proved that the photograph was taken on the date at the time and in the position so appearing.

In Art. 61 (3), the legislation lays down the information required to be given to support the authenticity of the photograph (see below).

(3) A Fisheries Officer who takes a photograph of the kind described in sub-section (1) may give a certificate appending the photograph stating–

(a) his name, address, official position, country of appointment, and provision under which the officer is appointed;

(b) the name and call sign, if known, of any fishing vessel appearing in the photograph;

(c) the model of the camera, watch or clock or other instruments supplying the date and time and the position fixing instrument and a declaration that the officer checked those instruments a reasonable time before and after the taking of the photograph and, if necessary, in accordance with sub-section (2)(b) and that they all appeared to be working correctly;

(d) the matters set out in sub-section (2)*(a)*;

(e) the accuracy of the fixing instrument used within specified limits; and

(f) the maximum possible distance and the direction of the subject of the photograph away from the camera at the time the photograph was taken.

3 The use of and interpretation of VMS tracking

3.1 Introduction

The use of VMS (Vessel Monitoring System) and AIS (Automatic Identification System) transmission signals ('pings') from both fishing vessels and reefers/carriers are a valuable record of the position and, speed which can be used to evaluate vessel activity. This record can be used as evidence in prosecutions.

The fitting of transmitting equipment (transponder/transceivers) to ships is required under the SOLAS Convention,[41] Regulation V/19 - *Carriage requirements for shipborne navigational systems and equipment.* The regulation requires that AIS is fitted aboard all ships of 300 GT and above that are engaged, or intended to be, in international sailing, cargo ships of 500 GT, and above, not engaged in international voyages, and all passenger ships irrespective of size.

> "AIS shall provide automatically to appropriately equipped shore stations, other ships and aircraft information, including the ship's identity, type, position, course, speed, navigational status and other safety-related information; receive automatically such information from similarly fitted ships; monitor and track ships; and exchange data with shore-based facilities"[42]

[41] International Convention for the Safety of Life at Sea, 1974.1184 UNTS 278

[42] ". AIS data is accessible through several online portals such as MarineTraffic, FleetMon, AISlive or Vessel Finder

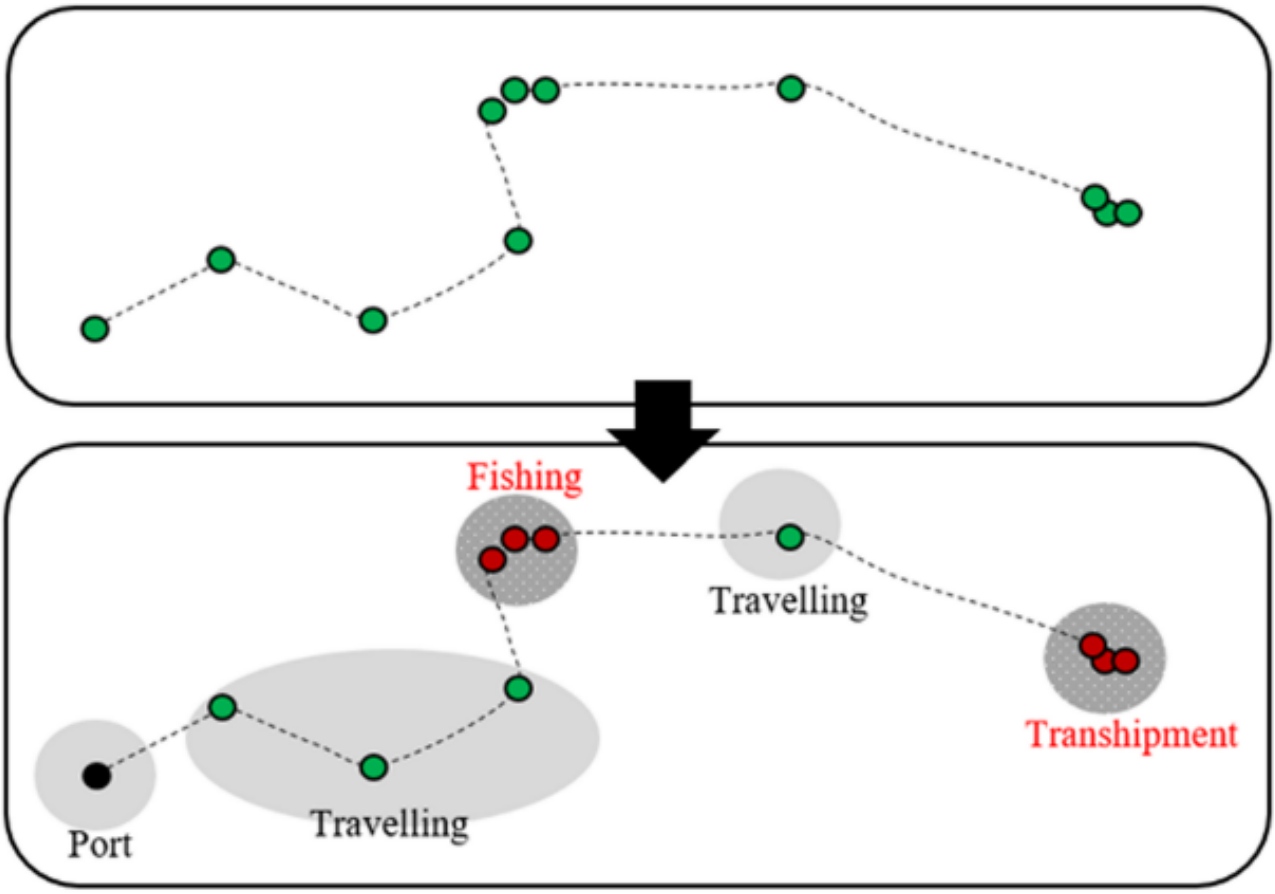
Individually, countries can then make regulations for AIS for vessels that are not covered by the SOLAS Regulation and that cover fishing vessels of lower tonnage.

A distinction needs to be drawn between VMS and AIS data. This distinction is essentially legal in that AIS transceivers are required to be carried in accordance with the SOLAS regulation V/19 and in accordance with the respective national regulations for fishing vessels. Although a number of states require that AIS is carried on fishing vessels, and there are regulations to ensure that these transmit continuously when at sea, not all fishing vessels are covered. VMS however implies that the fitted transceivers are subject to regulations for satellite monitoring since its signals can only be received by ground stations. By contrast, AIS is an 'open system', seen by other ships, and uses VHF radio in addition to satellite monitoring.

3.2 Use of VMS and AIS to determine fishing vessel activity

At its simplest, analysis of VMS/AIS tracks provide a clear and understandable history of a vessel's activity. The figure below demonstrates the basic movements and analysis of a fishing vessel at work over time,

Figure 13: Reconstructing vessel behaviour from GPS positions



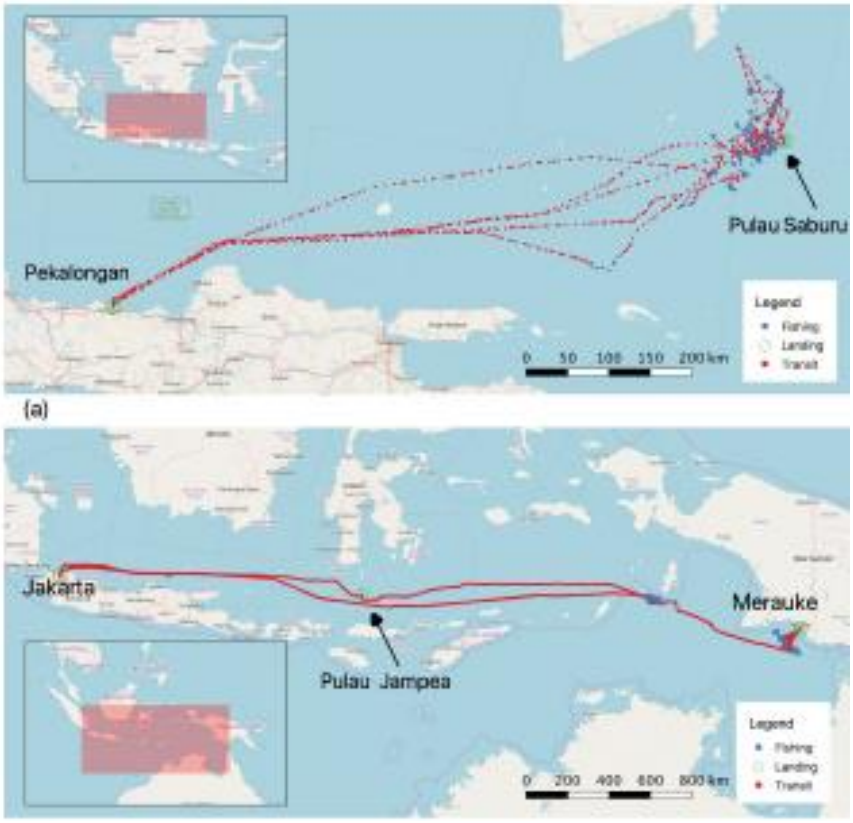
(Source: Chuaysi and Kiattisin [43])

[43] Buncha Chuaysi and Supaporn Kiattisin, 'Fishing Vessels Behavior Identification for Combating IUU Fishing: Enable Traceability at Sea' (2020) 115 Wireless Personal Communications 2971.

The figure speaks for itself but points to note are not only the straight line ‘legs ‘ when travelling, and then the closely spaced very short legs when fishing, as distinct from the tight packing of positions when transhipping, the movement being due to drift, caused by wind or current, in the sea.

Expert analysis can distinguish between the tracks made by different types of fishing vessel. Figure 14 shows the activity of two different types of vessel: a purse seiner and a squid-jigger. The purse -seiner[44] has a long track to its fishing ground, in the Makassar Strait. The track clearly shows the intense activity of its more complex fishing method, with more wide spaced stops to fish until it finds a more productive area. After fishing it return to its port in Pekalongan. The squid-jigger has a simpler track, with its fishing in the Arafura and Banda Seas, carried out during its journey to and from its port. Its track also shows the stop-off points before its return to Jakarta.[45]

.Figure 14: Comparison of purse-seine & squid-jigger



(Source: Feng Chi Hsu and others)

[44] Purse-seiners referred to in this section are SE Asian vessels generally fishing for small pelagics. Not to be confused with tuna purse-seiners

[45] Feng Chi Hsu and others, ‘Cross-Matching VIIRS Boat Detections with Vessel Monitoring System Tracks in Indonesia’ (2019) 11 Remote Sensing 1.

3.3 Detailed analysis of vessel tracks

The initial problem, with analysing a fishing trip set of tracks is that the analysts is presented with a confusing set of tracks as in Figure 15. Careful analysis can break down the trip into a set of individual 'routes' or fishing events. Figure 16 shows the individual fishing event. The figure shows the position transmission points with the long travel 'legs' being distinguished from the 'points of interest' where the concentrated activity demonstrates that fishing – or some other activity such as transhipping – is taking place, (the figures of detailed activity have been taken from Chuaysi and Kiattisin.[46])

Figure 15: Fishing trip - whole trip

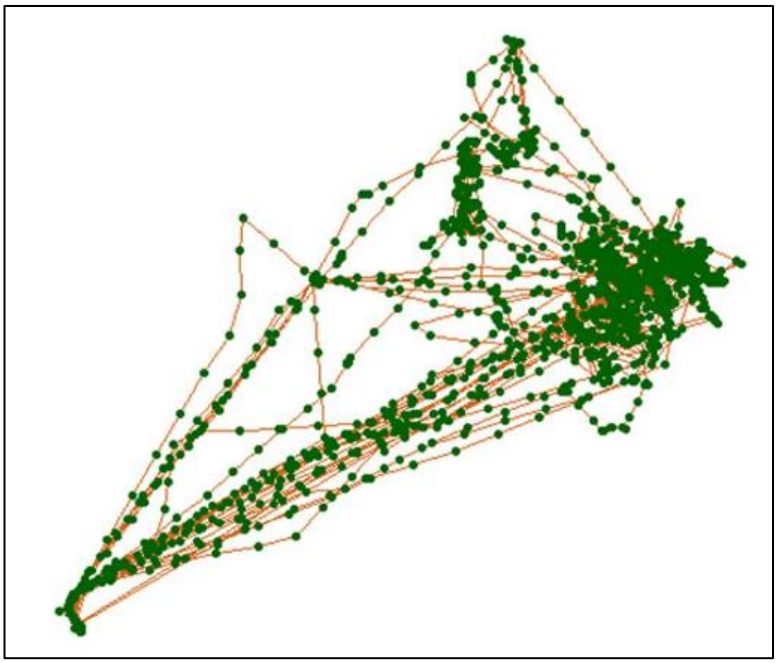
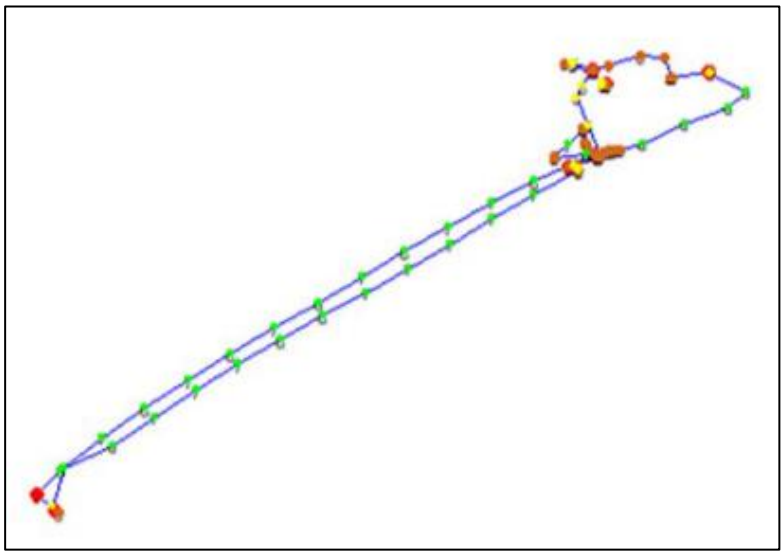
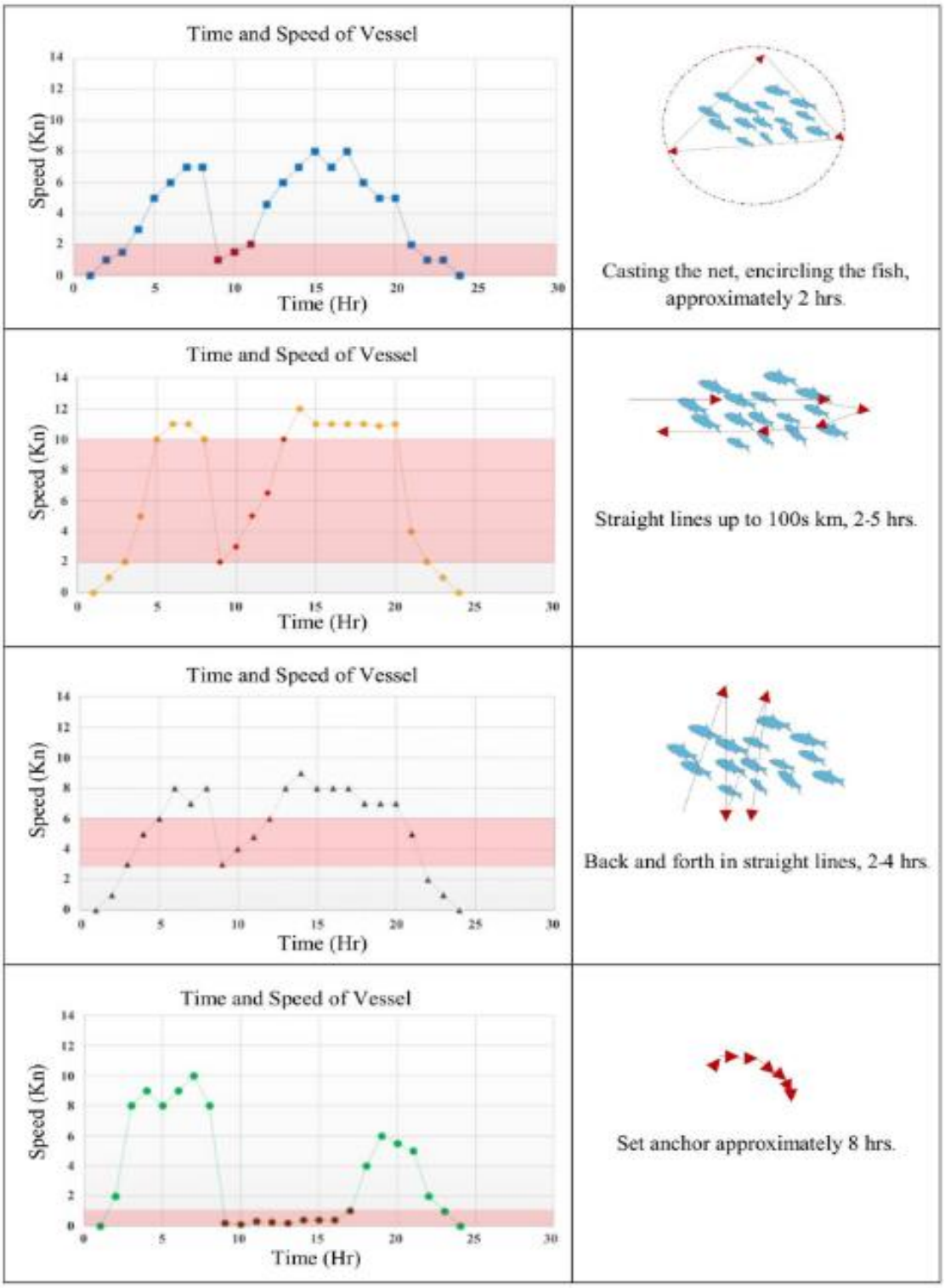


Figure 16: Individual fishing event



[46] Chuaysi and Kiattisin (n 41).

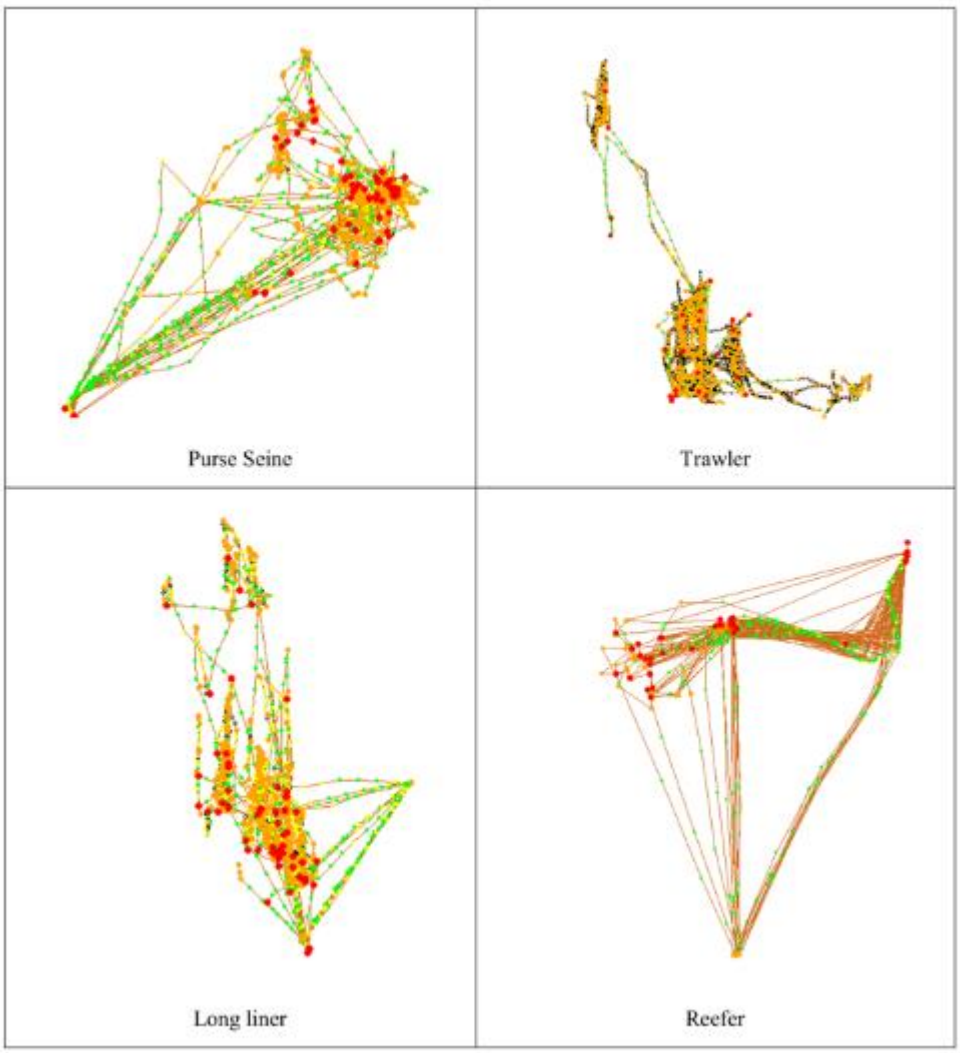
Figure 17 Detailed analysis of fishing activity by time and speed



More detailed analysis of speed and time points can be seen in Figure 17. This gives a very good breakdown of how a vessel moves in its fishing activity and that these movements are characteristic. What is characteristic of an individual fishing vessel's activity is also characteristic of particular types of fishing

as can be seen in Figure 18. In these examples, green dots show fast speed and red/yellow dots slower speeds with the red dots showing the slowest speeds.

Figure 18: Characteristic tracks of different types of fishing vessel compared with a carrier/reefer



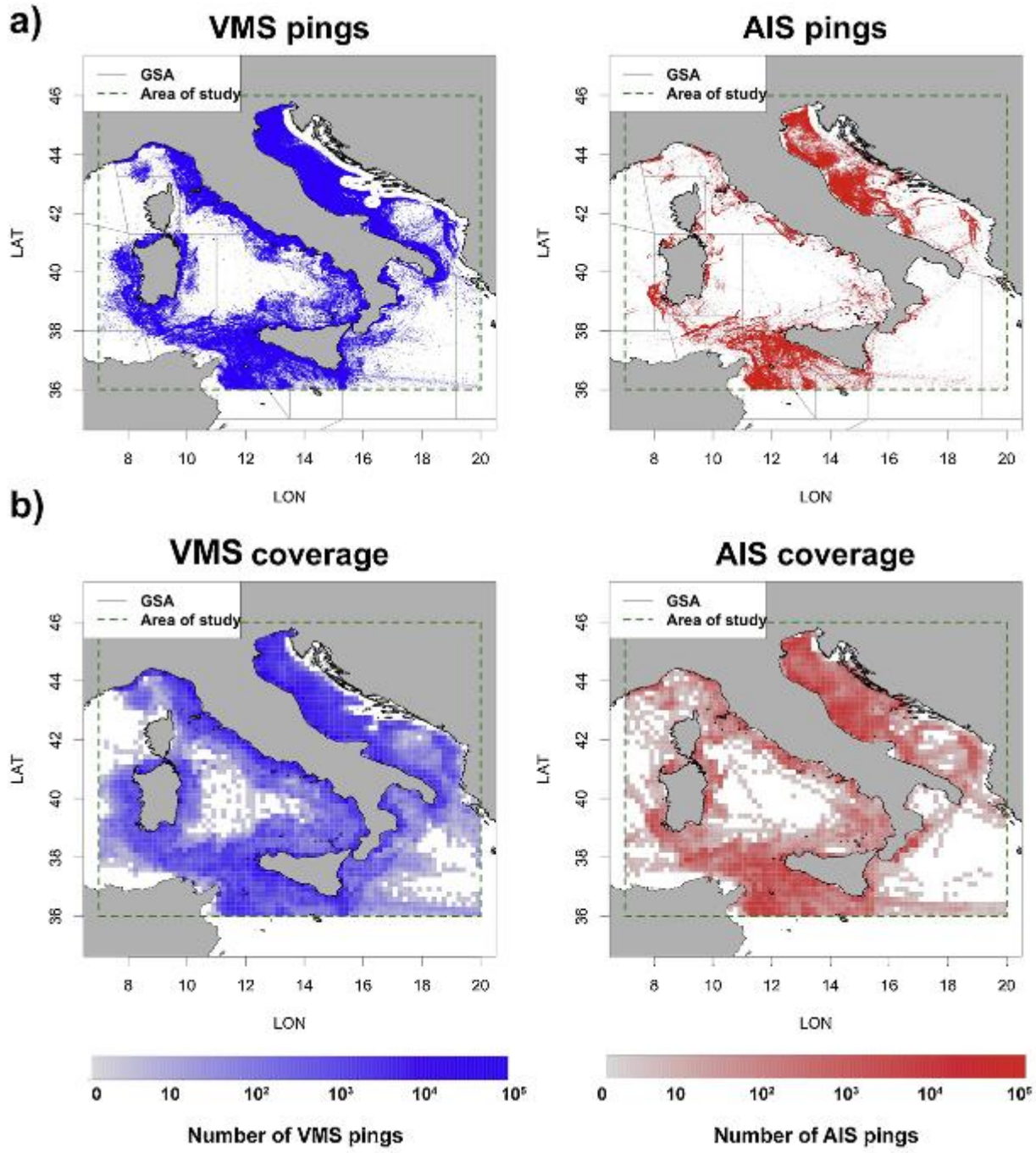
The tracks show both the journey legs, which are more pronounced with the carrier vessel. With the red dots indicating the transhipment points. The longliner also shows a characteristic of legs where the lines are shot, followed by the slower – 'red' – speeds where the line is hauled in and the catch taken off. Trawling also demonstrates lengthy slow 'red' legs (between 1 and 2 knots) with longer green legs between fishing grounds and ports.

3.4 Comparison of VMS with AIS

Figure 19 shows a comparison of VMS "pings" with AIS "pings" by fishing vessels in Italian waters.[47] The evidence is that AIS coverage appears to be less than VMS coverage. This lack of coverage becomes more critical with smaller vessels, meaning that not all areas can be covered

[47] T Russo and others, 'Assessing the Fishing Footprint Using Data Integrated from Different Tracking Devices: Issues and Opportunities' (2016) 69 Ecological Indicators 818 <http://dx.doi.org/10.1016/j.ecolind.2016.04.043>.

Figure 19: Comparison of transmission coverage between AIS and VMS

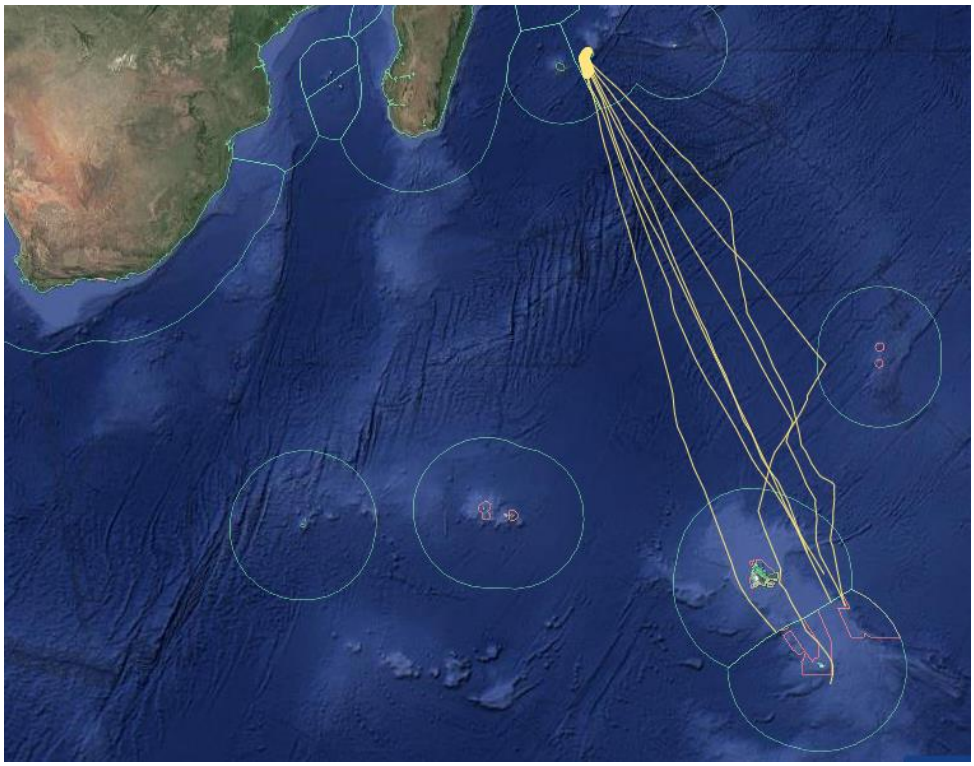


The loss of coverage needs to be considered not only in terms of national regulation but also in the ability to track vessels. This is important in the consideration of tracking the behaviour of carrier vessels and transhipments.

3.5 VMS and AIS transmission failure

VMS equipment that is fitted and governed by fisheries regulations can be deliberately turned off but to do so risks discovery and sanctions but AIS equipment when fitted, is generally governed by different and less stringent rules. Figure 20 shows the track record of an Australian commercial fishing vessel, operating out of Mauritius. The record shows that it appears that it has disabled its AIS on 10 separate occasions over a 12-month period when operating near the Heard Island and McDonald Islands Marine Reserve, in the Southern Ocean.[48] This loss of signal can be seen from the number of clear vessel tracks heading to and from the target area and which do not correspond to the very low number of identified tracks inside the target area

Figure 20: Disabled transmissions



Loss of signal from AIS – and VMS – transmitters is a very real problem with IUU, or potential IUU, fishing vessels. This problem can be overcome by systems that can make use of satellite radar imagery to determine ship positions by matching navigation or surveillance radar images and satellite images. An estimate of the radar image is generated using satellite or map image and the estimated radar image is compared with the real radar image. The new image is updated iteratively using an estimated ship position. By this means, the subsequent behaviour of the vessel can be evaluated.

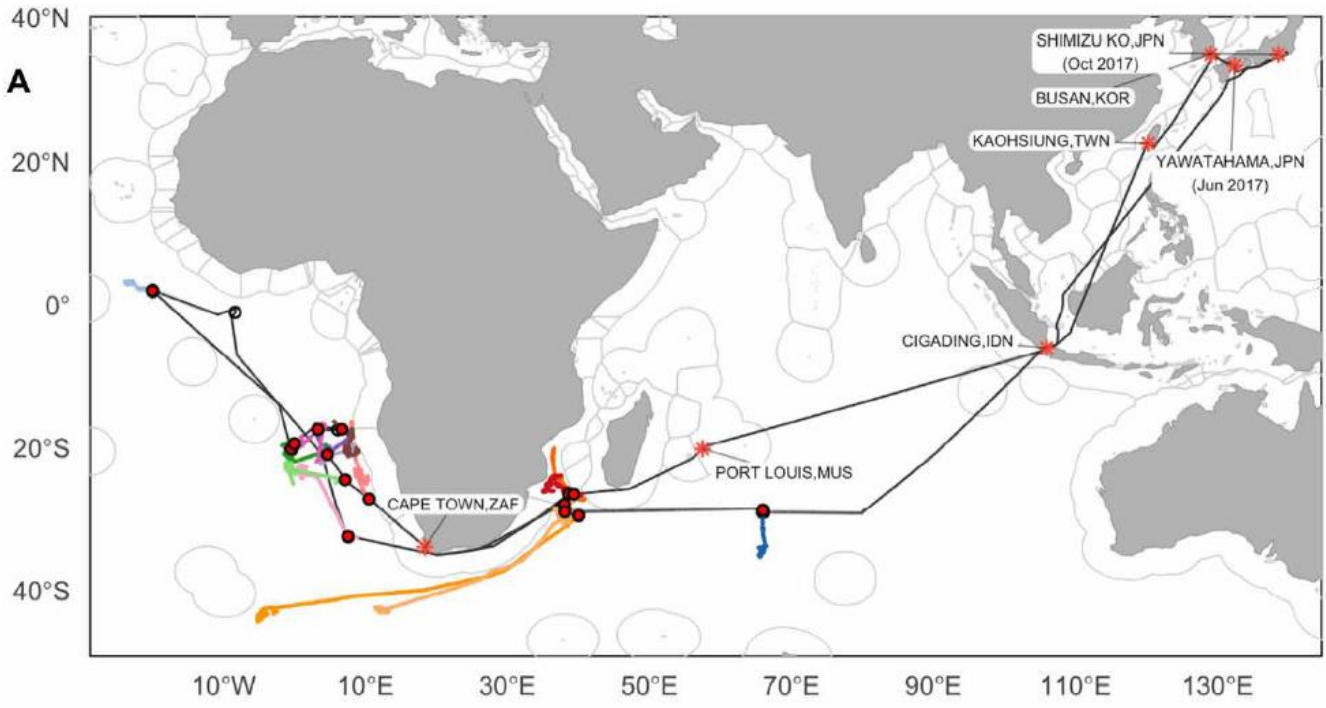
[48] https://globalfishingwatch.org/legacy-map/workspace/udw-v2-1518e343-8927-4b0b-b2d6-030ed4190a6f

3.6 Using tracking to identify transhipment behaviour

Transhipment is an important issue for IUU fishing since illegal catches can be transferred to a carrier at seas and then the same carrier can then use a port with limited, or absent or corrupt, inspection facilities to 'launder' its cargo so that it can enter the legitimate market and the legitimate market price: it becomes a value-adding operation. The problem for AMS wishing to protect their domestic export industries is that if Catch Data record – from IUU fish – enter the legitimate market or processing of products and are discovered, then the whole export industry becomes suspect. In such cases, the importing countries' inspections services are alerted to all imports from that States, with consequent delays and costs.

Tracking the behaviour of known carriers, therefore becomes of interest in the control of IUU access to legitimate markets. The following figures demonstrate the main routes and where transhipments are being made. Figure 21 shows the main transhipment points and the carrier routes for the Atlantic Ocean (opposite Namibia) and the Indian Ocean (between Mozambique and Madagascar) with the red dots indicating 'hot spots' for transhipment.

Figure 21: Overview of albacore transhipment



On the next page, Figure 22 (A) shows a record of a transhipment south of Madagascar. The fishing vessel is shown in blue and the carrier in purple. Note the distinctly different tracks shown by the fishing vessel and the carrier. The carrier shows long straight voyage 'legs', compared with the zig-zags and tightly bunched tracks of the fishing vessel, particularly south of Madagascar where there has obviously been a long period of intense fishing.

The close-up in Figure 22 (B) (the close-up -dotted box – is part of the intense fishing area) and shows how the two vessels align on a parallel path (inside the re dotted line in B). The distinction between the two patterns of behaviour – zig-zag against straight tracks – is a clear sign of the different types of activity between fishing and travelling to tranship. The only time the fishing vessel shows a long straight track is when it is aligned with the carrier so that transhipment can take place. These behavioural differences provide circumstantial evidence of transhipment

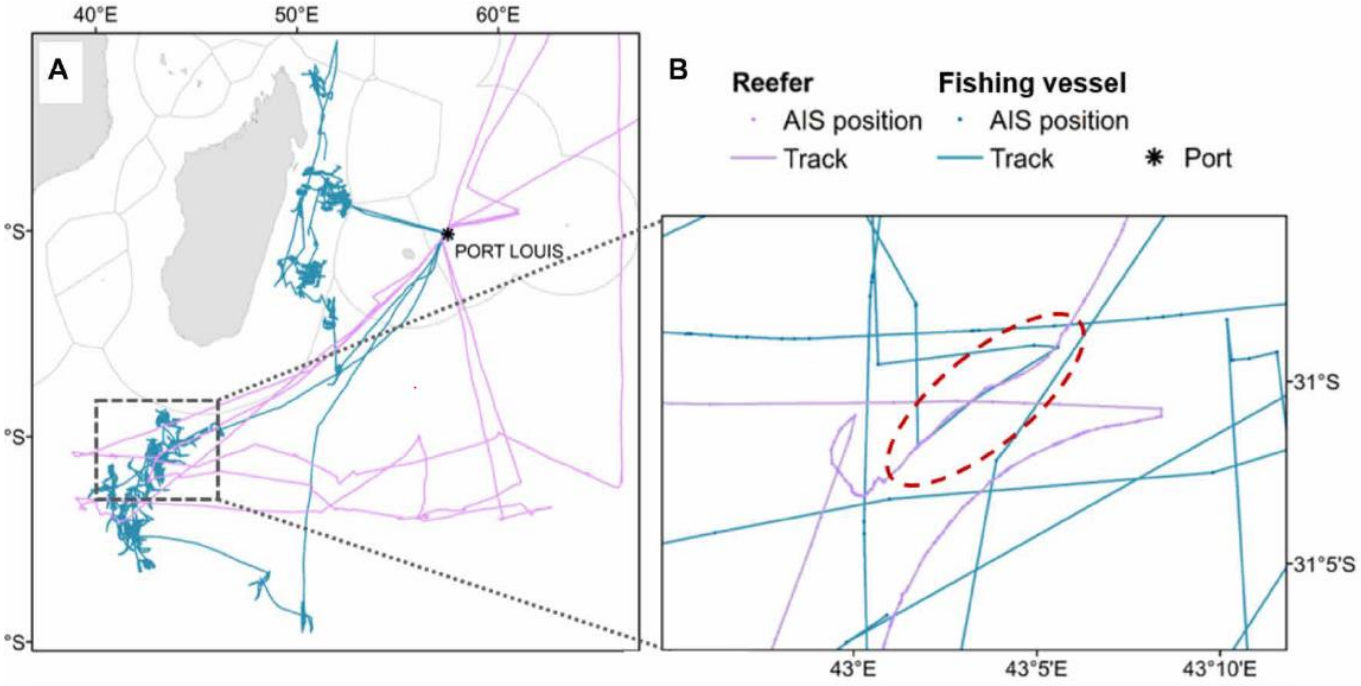


Figure 22: Close up of albacore transhipment

(Figures 21 and 22 in are taken from Boerder *et al*[49])

3.7 Using VMS/AIS tracks as evidence

The point to be made is that whether a vessel is fishing legally or not, its track will be characteristic of its type of activity – by fishing type or if it is transhipping. Because it is characteristic, then a track history can be presented to a court as direct evidence of its activity. It is direct evidence of the vessel's position since the 'ping' is automatic and can be recorded. However, there are a number of points which need to be made:

1) The transmitter needs to be certified as being a reliable transmitter of accurate data. This can be done by a technical expert when the vessel is in port.
2) The analysis of the tracks can only be given as expert opinion. The court may seek further opinions from other experts in its consideration of the evidence and will weigh each expert's opinion carefully.

There have been a number of cases brought to courts where prosecutions have been made using VMS data. In a recent case in the UK, the local inshore fisheries enforcement authority brought a prosecution against a trawler: in this instance, two experts were consulted by the court and a 'Not Guilty' verdict was reached by the jury.[50] The problem with this case is that the experts' opinion appeared to rely heavily on position, course, speed and direction. Over this the experts differed. The issue was whether or not the positions demonstrated that the vessel was actually fishing, or simply travelling:

The quote (from the case report [see Table 1, Case A]) below sums up the circumstances of the case

[49] Kristina Boerder, Nathan A Miller and Boris Worm, 'Global Hot Spots of Transshipment of Fish Catch at Sea' (2018) 4 Science Advances 1.
[50] Laura D Fishing Limited, South West Trawlers Limited and two private individuals, in respect of a prosecution brought by the Devon & Severn Inshore Fisheries & Conservation Authority ('D&SIFCA').

> "…unless a fisherman is caught in the act, these cases are often very difficult to prove and perhaps the decision to pursue the case was influenced by a desire to gauge the weight of VMS evidence in Court."

It should be understood that under English law, the value of expert opinion has been described as being:

> "The theoretical position is that experts are expected simply to educate the jury, to pass on the relevant aspects of their knowledge and expertise so that the jury itself can properly assess the evidence to which it relates."[51]

However, another case, in the USA, gave a different result [see Table 1, Case B]. In this case, the fishing vessel was independently tracked by both a control room and a coastguard vessel. Here the case was undoubtedly based on demonstrating clear intent by using the VMS data to demonstrate that the vessel has entered a closed area and that positions showed that it was not an ordinary passage. This case is interesting in that the use of VMS data to prosecute was also, as with the English case, above a first-time use of VMS data and also a test prosecution (to test whether VMS evidence would be accepted by a court). The convicted fisherman later appealed (twice) the decision, arguing that the use of VMS data, as a first-time test, constituted "a malicious prosecution"; the appeals failed.[52]

Table 1. VMS Evidence Case Reports

Case A: case report "...four Devon scallop fishermen faced prosecution at the Gloucester Crown Court for allegedly fishing within prohibited areas in the offshore limit in January and February 2016. The Devon and Severn Inshore Conservation Authority who have jurisdiction over this area brought the prosecution on the basis of VMS data received during that time. Whilst it was not denied, at the material time, the vessels were located in prohibited areas; the fishermen maintained that the fishing gear was not being used. Evidence of the prevailing sea and weather conditions were produced as being conducive to good fishing conditions, but the prosecution case ultimately relied upon VMS data. Although the vessels were fitted with Automatic Identification System (AIS), these were not in operation at the time and the Authority argued that this was a further attempt to conceal illegal fishing. Whilst evidence of speed, conditions and position are often suggestive of fishing activity, the intermittent readings by the VMS equipment alone were insufficient to prove that the fishermen had fished in prohibited areas and accordingly, they were acquitted. It was undoubtedly in the public interest to pursue such a case but with the level of reliance on VMS data, it is surprising that the Authority considered this to be sufficient to provide a realistic prospect of conviction.

[51] Law Commission, 'The Admissibility of Expert Evidence in Criminal Proceedings in England and Wales: Recapitulation and Review' (2009).
[52] 750 F.3d 100 (1st Cir. 2014), 13-1947, Yacubian v. United States

That said, unless a fisherman is caught in the act, these cases are often very difficult to prove and perhaps the decision to pursue the case was influenced by a desire to gauge the weight of VMS evidence in Court. It is important to convict the guilty but far more important to ensure the innocent are not convicted."[53]

Case B : case report:

The scallop vessel was tracked by the VMS from Dec. 9 to 11, 1998, as it made several incursions into an area closed to protect spawning groundfish approximately 160 nautical miles off the coast of Massachusetts. The initial VMS report put the vessel 1.36 nautical miles inside the area. Using radar and other onboard navigational systems, the U.S. Coast Guard Cutter Wrangell also tracked Independence inside the area and confirmed a second incursion. "This case sets an important precedent by holding that the VMS system in use on scallop vessels in the Northeast is an accurate, reliable technology capable of producing evidence of vessel activity admissible in a court of law," added Charles R. Juliand, lead NOAA prosecutor handling the case. Judge Bladen found that Independence repeatedly entered the closed area located approximately 160 nautical miles off the coast of Massachusetts. The judge also stated that, together with a significant monetary penalty, the removal of intentional violators would send a clear and loud message to the fishing industry that purposeful and sustained incursions into closed areas will bring meaningful sanctions. "The significance of this case was that the judge accepted VMS data as evidence that the vessel was inside the closed area," said Special Agent Louis Jachimcyzk of NOAA Fisheries Office for Law Enforcement, case agent for the IF/V Independence investigation. "This type of information had never been used, on its own, to prove a closed-area case."[54]

[53] https://www.williamsons-solicitors.co.uk/services/fishing-vessels-caution-to-be-exercised-with-vms-data/

[54] https://www.greenenvironmentnews.com/Environment/Climate/N.O.A.A.+Achieves+1st+Prosecution+Using+Satellite-based+Vessel+Monitoring+System

Educating a court in different circumstances, argues that more weight should be given to past history of activity, particularly for individual vessels. This approach means that in achieving a successful prosecution of a vessel, using tracks, it is necessary to:

1) Build up a good library of identified[55] vessel tracks that can be used to provide substantial supporting evidence of the behaviour of similar vessels;
2) Demonstrate, using track history, that the suspect vessel fitted the pattern of other vessels fishing (or transhipping) in similar circumstances.
3) Build up expertise in analysing vessel tracks within each AMS Fisheries Monitoring Centres, and also to access academic experts within each country.
4) Prosecutions using VMS/AIS tracking should be, where possible, supported with other evidence such as logbooks.

Readers should bear in mind that evidence of behaviour shown by tracking can only be regarded as circumstantial, unless the behaviour can be verified by visual evidence made at the same time i.e., by a patrol boat or patrol plane.

3.8 Confidentiality of VMS information

It has been argued strongly by the FAO Legal Office that VMS information should be treated as confidential because the information is commercial. Commercial fishing companies do not want to give away their vessels fishing behaviour and choice of fishing ground. If they feel that this information may be made public then there will be resistance to cooperating with fisheries authorities over VMS, Therefore, although it may be possible to track IUU vessels with VMS, unless the evidence is given in an open court, all such information should be treated as confidential. The Legal office advise that:

- VMS information is classified as confidential information;
- VMS information should be used primarily for fisheries management purposes;
- Any use of VMS information, other than its primary purpose, should be made explicit and detailed i.e. “for enforcement, search and rescue, and…”;
- Restricting access to the premises where the VMS information is generated, stored or processed to authorised persons and similarly for access to VMS information;
- To make breach of confidentiality an offence, punishable by severe penalties

If this cannot be achieved through legislation or regulation, then it is suggested that the intent of this advice could be achieved by specific terms in staff contracts or by making addenda to terms of employment to require staff to keep such VMS information confidential

3.9 Final word on the use of VMS and AIS tracking

This Section has discussed the use of VMS and AIS tracking as a record of vessel behaviour and how this could be used in enforcement: the technical means of analysing vessel tracking has not been discussed but examples have been presented to show its use. The importance of analysing this source of information has not been always been given the level of attention by Fisheries Monitoring Centres (FMCs) that it deserves. However, there is technical expertise available within the region, notably in Indonesia and Thailand (references are given) which could be made use of by fisheries enforcement. There is a good case for inviting such experts to offer training to FMC staff so that this expertise can be acquired and made use of. The analyses shown also indicate the value of FMCs being staffed by personnel with an understanding of and importantly, good experience of fishing activities so that track interpretation can be made more effective.

[55] Identified by name, IRCS and IMO number.

4 The international law for the arrest of fishing vessels

This section discusses international law as it relates to the arrest of fishing vessels, or more particularly, the arrest of vessels suspected of IUU fishing. Because the arrest of fishing vessels at sea often gives rise to contentious issues, and can often provoke the use of force, often inappropriately, it is important that there is a clear understanding of international law in this area. This section will concentrate on fisheries, and thus will not deal with piracy or narcotics but it does touch on slavery as this has some relevance to IUU fishing vessels and their crew conditions.

Also, within this section are a number of other legal issues which need to be considered:

- the meaning of misreporting and how it should be treated;
- the status of chartered vessels; and
- the treatment of any foreign fishermen arrested and convicted for a fisheries offence within the EEZ.

4.1 The meaning of 'hot pursuit'

(see: Agarwal[56]; Allen[57]; Molenaar[58]; Walker[59])

Hot pursuit' is covered by Art. 111 of UNCLOS. Put simply, 'hot pursuit' is actioned only when a vessel fails to stop, or makes a subsequent attempt to escape, following a legitimate order to stop, made by a properly authorised and recognisable enforcement vessel. The provisions are given below with the key elements noted in bold italics. The key elements will then be examined separately:

a) Hot pursuit may be initiated by the ***competent authorities*** [of the coastal state] (Art.111.1);
b) [Coastal State] must have "***good reason*** to believe" that the vessel has violated the laws and regulations of the state (Art.111.1);
c) Pursuit is of the offending "foreign ship or ***one of its boats***" (Art.111.1);
d) Pursuit can only start within the waters that the state has full jurisdiction over (internal waters, territorial sea, contiguous zone or archipelagic waters)[60] (Art.111.1);
e) Pursuit may be continued outside the jurisdictional waters (as above) PROVIDED that the chase is not interrupted;
f) Hot pursuit also applies to violations with the EEZ***, on the continental shelf***, including safety zones around continental shelf installations, including safety zones around any such installations (Art.111.2).
g) Hot pursuit must stop when the offending vessel enters the **TERRITORIAL SEA** (NB. not applicable to contiguous zone) **of its flag state OR the territorial sea of another state** (Art.111.3);
h) Hot pursuit can only be regarded as being started once the pursuing ship has "***satisfied itself by such practicable means*** as may be available" that

[56] Akash Agarwal, 'Critical Analysis of Doctrine of Hot Pursuit in Respect of Maritime Piracy' (2020) 2 International Journal Of Legal Science And Innovation 685.
[57] Craig H Allen, 'Doctrine of Hot Pursuit: A Functional Interpretation Adaptable to Emerging Maritime Law Enforcement Technologies and Practices' (1989) 20 Ocean Development and International Law 309.
[58] Eric Jaap Molenaar, 'Multilateral Hot Pursuit and Illegal Fishing in the Southern Ocean: The Pursuits of the Viarsa 1 and the South Tomi' (2004) 19 International Journal of Marine and Coastal Law 19.
[59] Randall Walker, 'International Law of the Sea : Applying the Doctrine of Hot Pursuit in the 21st Century' (2011) 9 Auckland University Law Review 194.
[60] In the rather special circumstances of the contiguous zone, then pursuit can only be initiated if the violation was of one of the rights for which the zone had been established. It should be noted that most contiguous zone restrictions relate to sanitary or customs regulations.

- the ship pursued (or ***one of its boats or other craft working as a team*** and using the ship pursued as a mother ship[61])";
- the ship pursued is within the ***limits*** of the territorial sea, contiguous zone or ***above the continental shelf*** (Art. 111.4);

- Hot pursuit starts only AFTER a ***visual OR auditory signal*** has been given (at a range or distance which those on the offending ship may be reasonably expected to see or hear) (art.111.4);
- Hot pursuit can only be carried out by a warship(s) or military aircraft or other ship and aircraft that are "clearly ***marked and identifiable***" as being on government service" and they must be ***authorised*** as such (Art. 111 5);
- When an aircraft carries out a pursuit then the rules above apply equally BUT, if the pursuing aircraft is unable to effect an arrest, then ***another ship or aircraft of the coastal state*** can make the arrest (Art. 111.6);
- The aircraft pursuing cannot make an arrest outside the territorial sea by simply sighting the offending vessel without the due cause for the violation being reasonable (Art. 111.6);
- Pursuit must be ***without interruption*** (Art. 111.6)
- Although a ship which has been wrongly arrested, following hot pursuit, may claim compensation (Art.111.8) a state cannot claim the release of its vessel by another state (the pursuing sate) which has arrested the vessel within its jurisdictional waters, by claiming that the arrested ship was crossing ***a portion of the EEZ or the high seas*** (Art.117).
  [Note: The terminology throughout this Article is to refer the 'ship or 'ships', not to the person or persons directing it. Under UNCLOS Art.94 (b) the flag state is required to ensure its vessels are in the charge of "a master and officers…"[62]

competent authorities

By the use of the term competent, UNCLOS does not mean competent to launch a vessel in pursuit but competent to judge whether or not a violation (of the relevant legislation or regulations) has taken place which would justify stopping the offending vessel. This is related to "good reason" (see below). Competence can also be extended to mean the authority, as invested through legislation, with the administrative and regulatory responsibility for the relevant area of concern i.e. the Department of Fisheries.

good reason

Good reason means that there is evidence of a violation having taken place. This means that the offending behaviour has either been sighted i.e. actually fishing, or that there is evidence of the offence, for example, an inspection might give evidence that fresh fish on board has been recently caught. Technical evidence of the offence would also provide "good reason" for example photographic evidence (especially if combined with a position fix), or radar or satellite tracks (see "practicable means").

one of its boats

[61] As in point c) on the preceding page
[62] This may create a difficulty, if not now, then in the future, with Marine Autonomous Vehicles (MAV).

"One of its boats" means that support craft, associated with a particular fishing vessel, may be subject to "hot pursuit", provided that the necessary procedures have taken place to establish "good reason" and a properly constituted stop order has been given. For example, if transhipment has taken place outside a port, contrary to national regulations, then both the fishing vessel and the carrier would be required to stop and, if either, or both, failed to stop then hot pursuit could be initiated.

on the continental shelf,

Use of the term "on the continental shelf", means that violations that would occasion a legitimate stop order, could include fishing, or some other such capturing of natural resources (e.g. 'sedentary species') found on the surface of the continental shelf. Since the extent of the continental shelf[63] may be outside the limit of the EEZ (see UNCLOS Art. 76), this would allow for a wider application of 'hot pursuit' to be broader than suggested by UNCLOS Art, The critical term here is "on" the continental shelf, since fishing in the sea above the continental shelf, outside the EEZ, but within the extended bounds of a claimed area of the continental shelf, would be legitimate fishing on the high seas.

It is, however, arguable, that fishing within the safety zone of an installation on the continental shelf, but outside the EEZ, might still constitute an offence capable of giving rise to hot pursuit. Fishing within such a zone being likely to be prohibited, in practical terms such an intervention may not be generally feasible since such safety zones tend to be no more than 500 metres around such an installation.

satisfied itself by such practicable means

"Satisfied itself by such practicable means" signifies that, using the tools and facilities available to it, the competent authority has evaluated the evidence of offending and has "good reason" to correctly identify the vessel to be pursued as being the offending vessel itself. "Practicable means" with respect to AIS or satellite tracking, argues that it is reasonable to assume, although this does not appear to have been tested, that track history, with interpretation (see Section **Error! Reference source not found.**), indicating normal passage, fishing, stopping for transhipment, should provide evidence of "good reason" to a court. Such evidence, presented to a court in a common-law jurisdiction, should be capable, of being given as evidence by certificate, providing the national legislation makes the necessary provision. In such a case, the certified evidence would then be accepted by a court as *prima facie* evidence rather than being treated as hearsay evidence.

Note: the start of the pursuit does not have to be immediate. It must be assumed that authority for the pursuit may need to be sought and approved. During this period the intending pursuer may continue to shadow the subject of the pursuit.

one of its boats or other craft working

This phrase means that support vessels or other fishing vessels when working as a fleet may be pursued if they are associated with the violation being responded to. This form of working together is known as 'constructive presence' and has important connotations as regards the 'mother ship'. The '#mother ship' can be seen to be the instigator (and the term implies that the support or team vessel habitually work with that ship) or leader of the associated vessels. This association (see Walker) may allow for hot pursuit of a vessel outside the jurisdictional zone because the original effect of that violation was felt within that zone.

visual OR auditory signal

[63] The precise bounds of the continental shelf, under Art. 76, are quite complex to determine and beyond the scope of these guidelines.

This is normally interpreted as meaning that the signal to stop (signal L [Lima][64]), possibly accompanied by signal K [Kilo][65]) should be given in such a way that the signal can be heard/seen with the reasonable expectation of comprehension on the part of the offending vessel. However, the wording of Art. 111.1 states that:

> *"It is not necessary that, at the time when the foreign ship within the territorial sea or the contiguous zone receives the order to stop, the ship giving the order should likewise be within the territorial sea or the contiguous zone."*

Meaning that the ship starting the pursuit need not be in the same zone, consequently, it has been argued that a radio message could be given by the pursuit vessel on the open channel – Channel 16. This message can be repeated, accompanied by the visual and auditory, signals as soon as the pursuit ship comes within the visual range of the vessel to be pursued.

marked and identifiable

Art.111.5 requires that the chase is carried out by military ships or aircraft or other ships (and aircraft). This allows civilian agencies to use their own craft to be pursuers but there should be clear signage to indicate their role[66] and national affiliation (flying the national civil ensign or departmental ensign). Art. 111.5 requires that the vessel should be authorised to that effect. This can be done by specific clauses in national legislation or by a legal notice (or authorising letter) issued by the relevant authority in the competent agency.

Continuous pursuit

Arts. 111.1 and 111.6 refer to pursuit being "without interruption". Writers on the subject are clear that the meaning of this is that the pursuit must be of the originally identified vessel (or its support craft) and that there should be no chance of the pursing vessel switching to pursue another vessel, through failing to keep a continuous watch of the pursued vessel. Although this concept has been interpreted by some writers as meaning that there should be a continuous visual watch, modern practice argues that radar pursuit, backed up by satellite tracking, should be acceptable. However, in the absence of AIS, the possible entry of the pursued vessel into a busy shipping lane, with numerous radar reflections creating 'clutter', within which the pursued vessel may be lost, argues that the preparedness for maintaining a visual watch should be an important factor for continuous pursuit.

Another ship or aircraft of the coastal state

In Art. 111.6 there is reference to "another ship or aircraft of the coastal state to effect the arrest" meaning that the original pursuit ship or aircraft does not need to be the arresting craft. This can be interpreted quite widely as there have been examples of hot pursuit where the actual arrest, made by authorised officers of the coastal state, has been made from a ship belonging to another country, marked as being on Government service of that country (see the arrest of the *South Tomi*[67]).

[64] "Stop immediately"
[65] "I wish to communicate with you"
[66] For example, displaying the word "Fisheries" on the upper parts of a fisheries patrol vessel.
[67] Trevor Gibson, 'The One That Didn't Get Away' [2001] Journal of the Australian Naval Institute 22.

Stopping hot pursuit

The entry of the pursued vessel into the territorial sea of its own or another country's territorial sea immediately stops the pursuit. Whether or not, the chase can be taken up again, should the pursued vessel leave the territorial sea, appears to be uncertain. It is arguable that if the pursued ship is effectively tracked, by radar or some other means, then the chase could be taken up on the basis that the entry territorial sea did not interrupt the chase since the ship remained identifiable. However, this would require very good evidence of "continuous sight" since, by failing this test, the interruption to continuous pursuit must hold good.

It is possible to continue hot pursuit with the agreement of the third country even when it is the flag state of the pursued vessel.

[*Note*: It is not clear if the 2016 Trilateral Cooperation Arrangement between Indonesia, Malaysia and the Philippines constitutes an arrangement that would permit pursuit of an IUU-fishing vessel into another state's waters.[68]]

In any event, a regional agreement on hot pursuit could provide a resolution to this issue.

4.2 Flag-hopping and Flags of Convenience

4.2.1 Flag-hopping

Flag-hopping is a not uncommon phenomenon in IUU fishing, particularly associated with the reaction of a suspect vessel to an attempt to board and inspect, leading, as might be expected, to a 'hot pursuit,' situation. The most usual form of action is that the inspecting vessel identifies a fishing vessel as either being an IUU-suspect or is suspected of fishing illegally and initially asks the suspect vessel for its registration details, licence and flag. A flag will be run up at the stern and the vessels registration (and license) will be checked with the vessel's flag being flown. The theoretical flag state will then reply that the vessel is either unknown to it or that a vessel of that name is no longer registered with it, On being informed of this, accompanied by an announcement of intention to board and inspect, the suspect vessel will then run up another flag, causing the inspecting vessel to send an information request to the new flag state. At this juncture, the suspect vessel will tend to attempt an escape, sometimes switching flags yet again *[69].

International law is clear on this subject, under Art. 92 of UNCLOS, a ship can only sail under one flag, including while in port. A change of flags is only allowed where there has been a "real" change of ownership or registry.[70] Under Art.92.2 A ship that sails under two flags may not claim nationality and is "assimilated to a ship without nationality". Consequently, such a ship is subject to the "right of visit" by a warship (see Section **Error! Reference source not found.** below)

[68] A regional agreement on hot pursuit could provide a resolution to this issue. Two possibilities suggest themselves (1) arrest could be made by a vessel of the other state; and (2) extension of a 'Lacey Act' form of agreement allowing arrest for an offence made in another territory, and treated as an offence as though made in the arresting state.

[69] Per-Erik Bergh, 'Ex-Togolese Fishing Vessel Changes Flag in the High Seas' (*Stop illegal fishing*, 2011) <https://stopillegalfishing.com/news-articles/ex-togolese-fishing-vessel-changes-flag-in-the-high-seas-4/> accessed 20 August 2020.

[70] There are exceptional circumstances, covered by specific treaties or within UNCLOS but these are highly specific.

4.2.2 Flags of convenience

Many, if not most, electively IUU-fishing vessels sail under flags of convenience. This is a particularly vexed subject since there is clear evidence that such states do not exercise the controls over their ships, envisaged by the 1993 Compliance Agreement;[71]. There is a considerable literature on this subject (see also Interpol[72]; Liddick;[73] Miller[74]). Under Art. 91.1 there must be a "genuine link" of nationality between the ship and the State to which it is registered. The frequent lack of any such link, particularly where the flag state is landlocked, means that the flag in such cases become effectively a legal fiction.

4.3 'Right of visit'

4.3.1 The right of visit and inspecting a ship

Warships have, under UNCLOS Art. 110, the "right of visit" which may *only* be exercised where there are is "reasonable ground for suspecting that":

> (a) the ship is engaged in piracy;
>
> (b) the ship is engaged in the slave trade;
>
> (c) the ship is engaged in unauthorized broadcasting and the flag State of the warship has jurisdiction under Article 109;
>
> (d) the ship is without nationality; or
>
> (e) though flying a foreign flag or refusing to show its flag, the ship is, in reality, of the same nationality as the warship."

Based on the above, the warship may send a boat with a boarding party to check the ship's documents and carry out further checks - on piracy, slavery and the proper nationality of the ship. The right to visit does not allow more than the inspection of documents. It is feasible to take action on piracy, but it is not clear that this would extend to slavery or slave-like conditions of crews onboard fishing vessels.

4.3.2 Definition of warship

Warships are defined under Art.29 of UNCLOS as being a vessel of the armed forces of the State, and marked as such, commanded by a commissioned officer, listed in the relevant service list of the State. For the purpose of the "right to visit", the right may also be exercised by military aircraft of the state, and by "other duly authorized ships or aircraft clearly marked and identifiable as being on government service", meaning that properly marked fisheries department vessels can also exercise this right.

4.4 Miscellaneous legal issues

There are a number of legal issues which are not clearly delineated, and which should be considered by the ASEAN Community. These issues are:

---

[71] [FAO] Agreement to Promote Compliance with International Conservation and Management Measures by Fishing Vessels on the High Seas, 24 Nov., 1993, 33 I.L.M. 968 (1994)

[72] North Atlantic Fisheries Intelligence Group and INTERPOL., 'Chasing Red Herrings: Flags of Convenience and the Impact on Fisheries Crime Law Enforcement' (2017) <https://fishcrime.com/wp-content/uploads/2017/09/Chasing-Red-Herrings-Report-Email.pdf>.

[73] Don Liddick, 'The Dimensions of a Transnational Crime Problem: The Case of IUU Fishing' (2014) 17 Trends in Organized Crime 290.

[74] Dana D Miller and U Rashid Sumaila, 'Flag Use Behavior and IUU Activity within the International Fishing Fleet: Refining Definitions and Identifying Areas of Concern' (2014) 44 Marine Policy 204.

4.4.1 Misreporting.

The definitions above there expand the range of reporting requirements. A vessel's logbook or other records of fishing, including attracting fish, or support activity (transhipping, transporting or bunkering) therefore comes within the ambit of reportable activities. This either not reporting on these activities or misreporting them becomes an IUU activity.

Misreporting would include all those things defined as fishing that are not permitted within national legislation as well as a counter to RFMO CCMs. These then likewise apply to support vessels and their actions. The issue of non-reporting of by-catch, or non-target species, is dependent on the framing of national legislation. RFMO CCMs are very explicit in this regard.

National laws which control and manage inland fisheries are therefore covered as also are the CCMs of the Mekong River Commission (MRC) as an appropriate regional RFMO.

However, the 2002 Expert Consultation suggested that 'mis-reporting'' should be re-defined as 'non-reporting'. This removes the position where a genuine error in reporting is treated as an offence, and instead misreported is redefined as a deliberate act either not to report or to falsify a report. It is suggested that this approach is reflected in national legislation.

4.4.2 Chartering and nationality

Chartering creates issues with how fishing vessels are regarded in international law, not least with 'rules of origin' in relation to fish exports. Lack of clarity over the chatter status of a vessel can cause problems with enforcing rules. For example:

- Vessel *Abc* is owned by a company operating (and registered in) Country X, BUT
- The *Abc* is registered – and thus flagged – by State Y; BUT
- The *Abc* has a permit to fish in the waters of Country Z

The skipper may not be a national of any of these states. This creates a problem for State Z as to any authorisation to board and inspect.

Another issue that may arise is when:

> The *Abc* is registered in State X but chartered by a company registered in State Y to fishing in the waters of Y as well as on the high seas. It is clear that while operating in the waters of State Y, then Y, as the coastal state, has the responsibility over the actions of the *Abc*. But, when on the high seas, State X, as the flag state, has responsibility but State Y no longer has any authority over the vessel. At the same time, State X may have no knowledge of where the *Abc* is operating.

The recommendation is to clarify chartering rules in national legislation. Two options are suggested:

1) Any foreign vessel being chartered by a national company to fishing in the waters of its own state as well as on the high seas, then that vessel should be required to be re-flagged to the flag of the company operating the charter.
2) If the countries involved are contiguous states then, those countries could enter into an agreed system for reciprocal inspection and boarding over vessels flying their flags.

4.4.3 Considerations over the application of national law in cases of IUU fishing

It should be noted that with regard to the definition of "Illegal", whether an infringement or contravention of fisheries regulations constitutes a crime (liable to a criminal /sanctions) or is subject to a civil or administrative sanction is irrelevant. However, with regard to penal offence, the issue of determining a vessel to be actively fishing because it has not stored its gear so as to make it unusable has international Human rights law implications (the Presumption of Innocence until proven to be guilty i.e. reversing the burden of proof).[75]

In determining penalties for any foreign crews of an arrested vessel, the terms of UNCLOS are clear:

> *Article 73: Enforcement of laws and regulations of the coastal State*
>
> 4. Coastal State penalties for violations of fisheries laws and regulations in the exclusive economic zone may not include imprisonment, in the absence of agreements to the contrary by the States concerned, or any other form of corporal punishment.

It should be clear that Art. 73 refers to fishers convicted of fisheries offences committed within the EEZ. This means that this article does not apply to offences committed within the territorial sea (or contiguous zone, where this may exist) or internal waters of the coastal state. It is equally clear that resisting arrest or offering violence when resisting arrest can only be treated as fisheries violations, provided they are covered by national fisheries legislation. In the case that violence is offered during an attempted arrest while the offending vessel is in the coastal state's territorial waters, and the vessel then escapes into the EEZ and thence into the high sea, then hot pursuit may commence (see Section **Error! Reference source not found.**). In the event of an arrest, after a successful hot pursuit, then the person offering violence, would be liable to prosecution, under the fisheries legislation (or regulations) or possibly the criminal code, insomuch as this may apply.

4.4.4 Use of force

A discussion of the legal basis for the use of force in fisheries would not be appropriate to these Guidelines, however, the point should be made that the legal issues discussed above do not necessarily fall within the scope of the use of force. In general, the use of force in fisheries is not seen as being necessary since fishing is a commercial activity, which does not fall into the same category as piracy, armed robbery or narcotics.

The basic principles governing the use of force in fisheries are given under Art.22.(f) of the FSA:

> "(f) avoid the use of force except when and to the degree necessary to ensure the safety of the inspectors and where the inspectors are obstructed in the execution of their duties. The degree of force used shall not exceed that reasonably required in the circumstances."

Art. 11 UN General Assembly, Universal Declaration of Human Rights, 10 December 1948, 217 A (III)

[75] Art. 11 UN General Assembly, Universal Declaration of Human Rights, 10 December 1948, 217 A (III)

(see also Freestone, David. & Food and Agriculture Organization of the United Nations. 1998, *The burden of proof in natural resources legislation : some critical issues for fisheries law FAO Legislative Paper No. 63/ by David Freestone* FAO Rome

There may be situations, including during hot pursuit, when the use of weapons may be considered necessary but international case law continues to regard the use of armed force as an absolute last resort (See *I'm Alone*,[76] *Red Crusader*[77] and *MV Saiga*[78]), In the case of the *MV Saiga*, the Tribunal[79] held that

> "It is only after appropriate actions fail that the pursuing vessel may, as a last resort, use force. Even then, the appropriate warning must be issued to the ship and all efforts should be made to ensure that life is not endangered."

Member States will have, of course, developed their own policies and rules of engagement in this matter.

[76] I'm Alone, Case. Canada vs United States, 1935, Report of Commission of Inquiry, 7 ILR 203-206

[77] Report of the Anglo-Danish Commission of Inquiry, 35 ILR 485

[78] The M/V 'SAIGA' (No 2), Saint Vincent and the Grenadines v Guinea, Merits, Judgment, ITLOS Case No 2, ICGJ 336 (ITLOS 1999), 1st July 1999, International Tribunal for the Law of the Sea [ITLOS]

[79] International Tribunal for the Law Of the Sea (ITLOS)